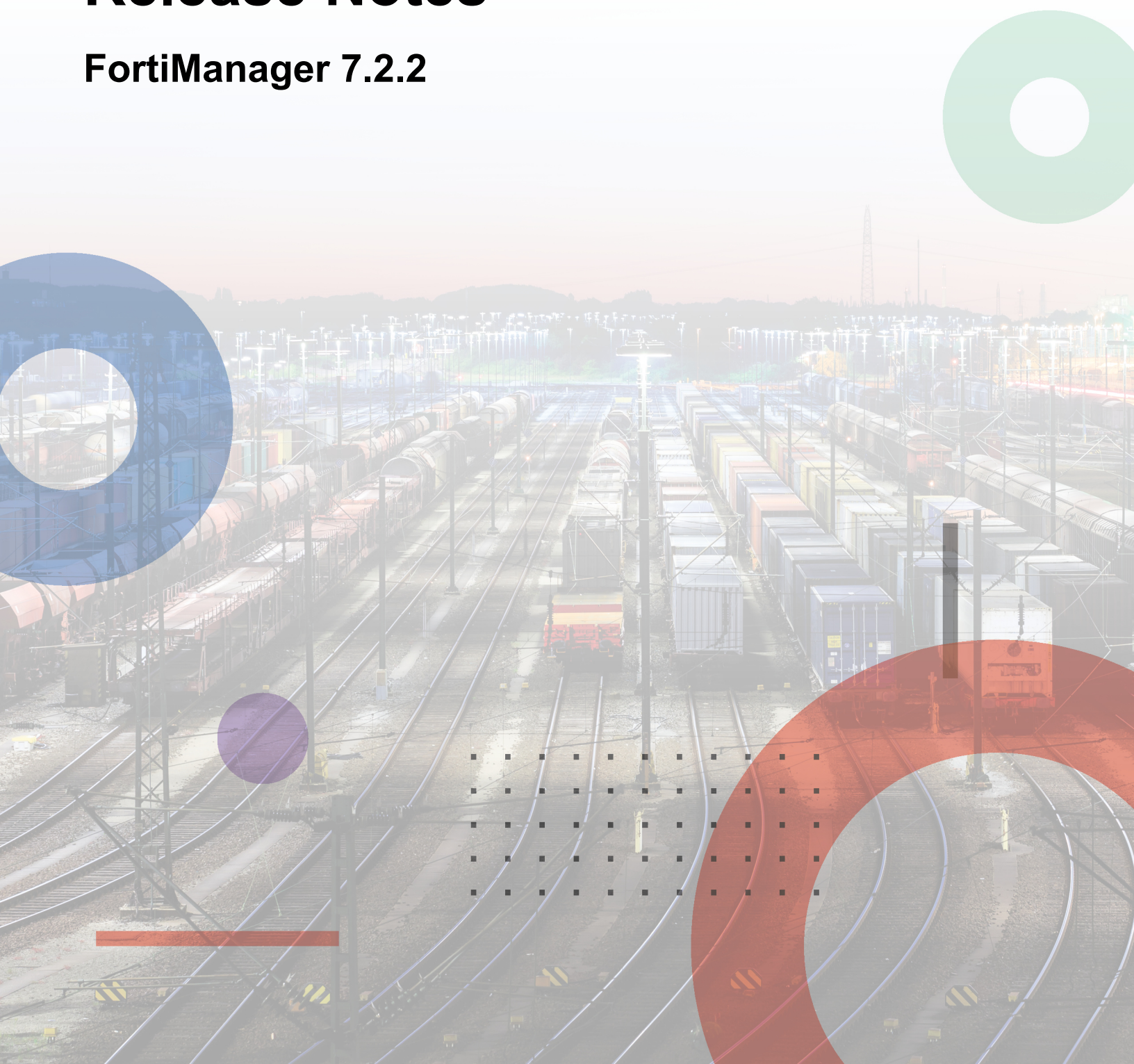
FORTINET

Release Notes

FortiManager 7.2.2



FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

May 18, 2023
FortiManager 7.2.2 Release Notes
02-722-839060-20230518

TABLE OF CONTENTS

Change Log

Date	Change Description
2023-02-02	Initial release.
2023-02-06	Added 881148 to Known Issues on page 56.
2023-02-07	Updated Special Notices on page 10.
2023-02-14	Updated FortiGate special branch models on page 28.
2023-02-21	Updated Virtualization on page 23 and FortiAnalyzer models on page 33.
2023-02-23	Updated 784385 in Known Issues on page 56. Added the workaround in Special Notices on page 10.
2023-03-03	Added FortiManager 7.2.2 and FortiOS 7.0.10 compatibility issues on page 39 Updated Resolved Issues on page 41 and Known Issues on page 56.
2023-03-08	Added FortiManager 7.2.2 and FortiOS 6.4.12 compatibility issues on page 39.
2023-03-14	Updated Known Issues on page 56.
2023-03-23	Updated FortiProxy on page 22.
2023-03-27	Added FortiManager 7.2.2 and FortiOS 7.0.11 compatibility issues on page 39.
2023-04-04	Updated Resolved Issues on page 41 and Known Issues on page 56.
2023-04-12	Updated Known Issues on page 56.
2023-04-17	Updated • Resolved Issues on page 41 • Known Issues on page 56 • FortiManager 7.2.2 and FortiOS 7.0.11 compatibility issues on page 39
2023-04-28	Updated FortiManager 7.2.2 and FortiOS 7.0.11 compatibility issues on page 39.
2023-05-04	Updated FortiProxy on page 22.
2023-05-12	Updated Resolved Issues on page 41 and Known Issues on page 56.
2023-05-18	Updated Resolved Issues on page 41 and Known Issues on page 56.

FortiManager 7.2.2 Release

This document provides information about FortiManager version 7.2.2 build 1334.

The recommended minimum screen resolution for the FortiManager GUI is 1920 x 1080. Please adjust the screen resolution accordingly. Otherwise, the GUI may not display properly.

This section includes the following topics:

Supported models

FortiManager version 7.2.2 supports the following models:

FortiManager	FMG-200F, FMG-200G, FMG-300F, FMG-400E, FMG-400G, FMG-1000F, FMG-2000E FMG-3000F, FMG-3000G, FMG-3700F, and FMG-3700G.
FortiManager VM	FMG_DOCKER, FMG_VM64, FMG_VM64_ALI, FMG_VM64_AWS, FMG_VM64_AWSOnDemand, FMG_VM64_Azure, FMG_VM64_GCP, FMG_VM64_IBM, FMG_VM64_HV (including Hyper-V 2016, 2019), FMG_VM64_KVM, FMG_VM64_OPC, FMG_VM64_XEN (for both Citrix and Open Source Xen).

FortiManager VM subscription license

The FortiManager VM subscription license supports FortiManager version 6.4.1 and later. For information about supported firmware, see FortiManager VM firmware on page 17.

See also Appendix B - Default and maximum number of ADOMs supported on page 63.

Management extension applications

The following section describes supported models and minimum system requirements for management extension applications (MEA) in FortiManager7.2.2.

FortiManager uses port TCP/443 or TCP/4443 to connect to the Fortinet registry and download MEAs. Ensure that the port is also open on any upstream FortiGates. For more information about incoming and outgoing ports, see the FortiManager 7.0 Ports Guide.

Supported models for MEA

You can use any of the following FortiManager models as a host for management extension applications:

FortiManager	FMG-3000F, FMG-3000G, FMG-3700F, and FMG-3700G.
FortiManager VM	FMG_DOCKER, FMG_VM64, FMG_VM64_ALI, FMG_VM64_AWS, FMG_VM64_AWSOnDemand, FMG_VM64_Azure, FMG_VM64_GCP, FMG_VM64_IBM, FMG_VM64_HV (including Hyper-V 2016, 2019), FMG_VM64_KVM, FMG_VM64_OPC, FMG_VM64_XEN (for both Citrix and Open Source Xen).

Minimum system requirements

By default FortiManager VMs use the following system resource settings:

- 4 vCPU
- 8 GB RAM
- 500 GB disk space

Starting with FortiManager 7.0.0, RAM and CPU is capped at 50% for MEAs. (Use the `config system docker` command to view the setting.) If FortiManager has 8 CPUs and 16 GB RAM, then only 4 CPUs and 8 GB RAM are available to MEAs by default, and the 4 CPUs and 8 GB RAM are used for all enabled MEAs.

Some management extension applications have minimum system requirements that require you to increase system resources. The following table identifies the minimum requirements for each MEA as well as the recommended system resources to function well in a production environment.

MEA minimum system requirements apply only to the individual MEA and do not take into consideration any system requirements for resource-sensitive FortiManager features or multiple, enabled MEAs. If you are using multiple MEAs, you must increase the system resources to meet the cumulative need of each MEA.

Management Extension Application	Minimum system requirements	Recommended system resources for production*
FortiAIOps	• 8 vCPU • 32 GB RAM • 500 GB disk storage	No change
FortiSigConverter	• 4 vCPU • 8 GB RAM	No change
FortiSOAR	• 4 vCPU • 8 GB RAM • 500 GB disk storage	• 16 vCPU • 64 GB RAM • No change for disk storage

Management Extension Application	Minimum system requirements	Recommended system resources for production*
Policy Analyzer	• 4 vCPU • 8 GB RAM	No change
Universal Connector	• 1 GHZ vCPU • 2 GB RAM • 1 GB disk storage	No change
Wireless Manager (FortiWLM)	• 4 vCPU • 8 GB RAM	No change

*The numbers in the *Recommended system resources for production* column are a combination of the default system resource settings for FortiManager plus the minimum system requirements for the MEA.

Special Notices

This section highlights some of the operational changes that administrators should be aware of in 7.2.2.

FortiManager creates faulty dynamic mapping for VPN manager interface during PP import

If policy changes are made directly on the FortiGates, the subsequent PP import creates faulty dynamic mappings for VPN manager.

It is strongly recommended to create a fresh backup of the FortiManager's configuration prior to this workaround. Perform the following command to check & repair the FortiManager's configuration database:

```
diagnose cdb check policy-packages <adom>
```

After executing this command, FortiManager will remove the invalid mappings of vpnmgr interfaces.

SAML SSO user: Retrieve, refresh, install, and device authorization fails from GUI after upgrade

If you are using SAML SSO with FortiManager, you must set the *rpc-permit* to *read-write* for SSO users on the service provider (SP) FortiManager.

If the *rpc-permit* is not set to *read-write* for SSO users, retrieve, refresh, install, and device authorization will fail from the GUI following the upgrade.

SD-WAN Orchestrator removed in 7.2

Starting in 7.2.0, the SD-WAN Orchestrator is no longer available in FortiManager. Instead, you can use the *SD-WAN Overlay Template* wizard to configure your SD-WAN overlay network.

For more information, see SD-WAN Overlay Templates in the FortiManager Administration Guide.

Changes to FortiManager meta fields

Beginning in 7.2.0, FortiManager supports policy object metadata variables.

When upgrading from FortiManager 7.0 to 7.2.0 and later, FortiManager will automatically create ADOM-level metadata variable policy objects for meta fields previously configured in System Settings that have per-device mapping

configurations detected. Objects using the meta field, for example CLI templates, are automatically updated to use the new metadata variable policy objects.

Meta fields in *System Settings* can continue to be used as comments/tags for configurations.

For more information, see ADOM-level meta variables for general use in scripts, templates, and model devices.

Setup wizard requires FortiCare registration

Starting in FortiManager 7.2.1, the FortiManager Setup wizard requires you to complete the *Register with FortiCare* step before you can access the FortiManager appliance or VM. Previously the step was optional.

For FortiManager units operating in a closed environment, contact customer service to receive an entitlement file, and then load the entitlement file to FortiManager by using the CLI.

Access lists as ADOM-level objects

Starting in 7.2.0, FortiManager supports IPv4 and IPv6 access lists as ADOM-level object configurations from FortiGate. Previously, access lists were controlled by the device database/FortiGate configuration.

After upgrading to 7.2.0 from an earlier release, the next time you install changes to a FortiGate device with an IPv4 or IPv6 access list, FortiManager will purge the device database/FortiGate configuration which may have previously contained the access list. To address this, administrators can re-import the FortiGate policy configuration to an ADOM's policy package or re-create the IPv4/IPv6 access list in the original package.

View Mode is disabled in policies when policy blocks are used

When policy blocks are added to a policy package, the *View Mode* option is no longer available, and policies in the table cannot be arranged by *Interface Pair View*. This occurs because policy blocks typically contain policies with multiple interfaces, however, *View Mode* is still disabled even when policy blocks respect the interface pair.

Reconfiguring Virtual Wire Pairs (VWP)

A conflict can occur between the ADOM database and device database when a Virtual Wire Pair (VWP) is installed on a managed FortiGate that already has a configured VWP in the device database. This can happen when an existing VWP has been reconfigured or replaced.

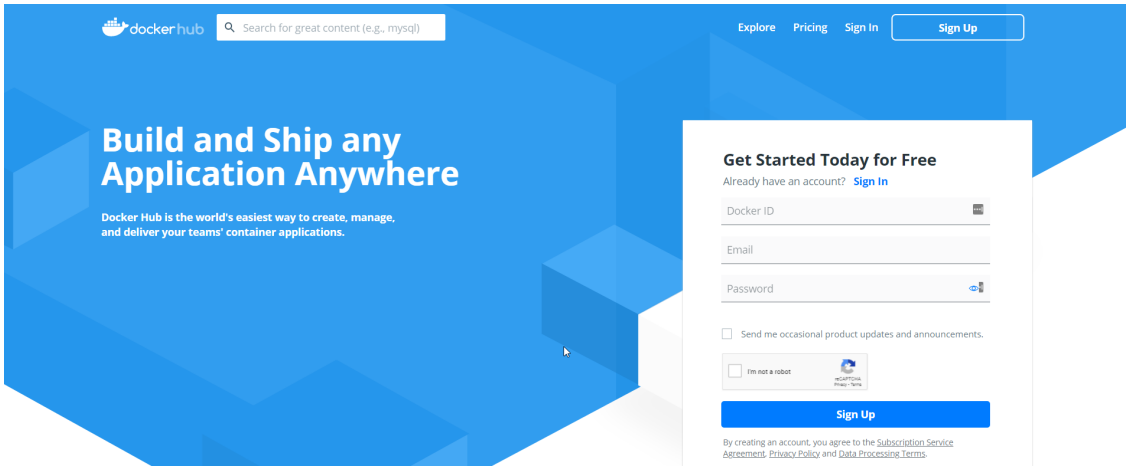
Before installing the VWP, you must first remove the old VWP from the device's database, otherwise a policy and object validation error may occur during installation. You can remove the VWP from the device database by going to *Device Manager* > *Device & Groups*, selecting the managed device, and removing the VWP from *System* > *Interface*.

Fortinet verified publisher docker image

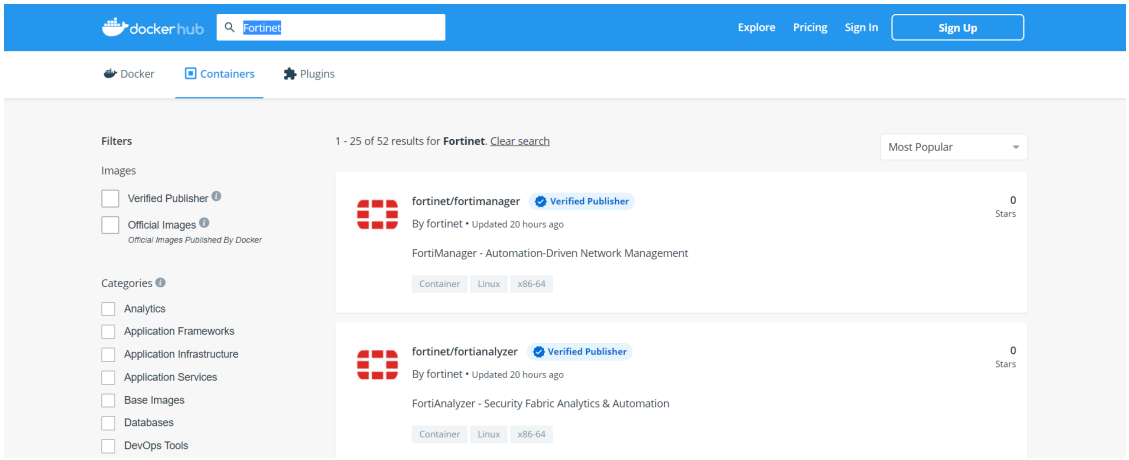
FortiManager docker images are available for download from Fortinet's Verified Publisher public repository on dockerhub.

To download the FortiManager image from dockerhub:

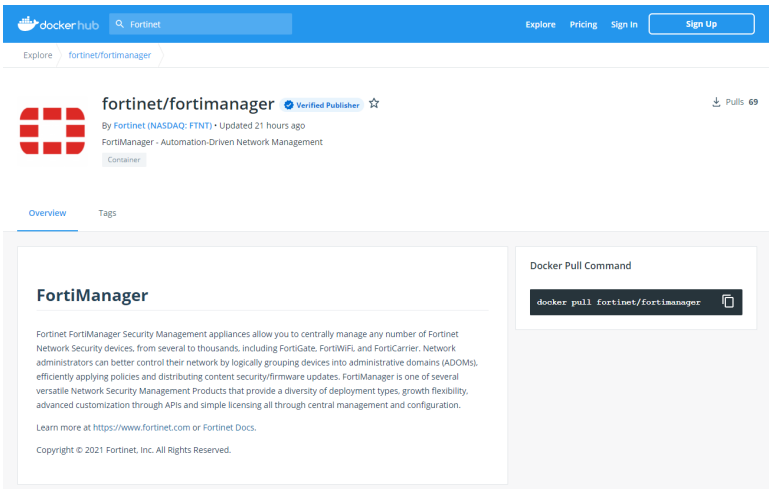
1. Go to dockerhub at https://hub.docker.com/.
   The dockerhub home page is displayed.



2. In the banner, click *Explore*.
3. In the search box, type *Fortinet*, and press *Enter*.
   The *fortinet/fortimanager* and *fortinet/fortianalyzer* options are displayed.



4. Click *fortinet/fortimanager*.
   The *fortinet/fortimanager* page is displayed, and two tabs are available: *Overview* and *Tags*. The *Overview* tab is selected by default.



5. On the *Overview* tab, copy the docker pull command, and use it to download the image.
   The CLI command from the *Overview* tab points to the latest available image. Use the *Tags* tab to access different versions when available.

Scheduling firmware upgrades for managed devices

Starting in FortiManager 7.0.0, firmware templates should be used to schedule firmware upgrades on managed FortiGates. Attempting firmware upgrade from the FortiManager GUI by using legacy methods may ignore the *schedule upgrade* option and result in FortiGates being upgraded immediately.

Modifying the interface status with the CLI

Starting in version 7.0.1, the CLI to modify the interface status has been changed from `up`/`down` to `enable`/`disable`.

For example:

```
config system interface
   edit port2
      set status <enable/disable>
   next
end
```

SD-WAN with upgrade to 7.0

Due to design change with SD-WAN Template, upgrading to FortiManager 7.0 may be unable to maintain dynamic mappings for all SD-WAN interface members. Please reconfigure all the missing interface mappings after upgrade.

Citrix XenServer default limits and upgrade

Citrix XenServer limits ramdisk to 128M by default. However the FMG-VM64-XEN image is larger than 128M. Before updating to FortiManager 6.4, increase the size of the ramdisk setting on Citrix XenServer.

To increase the size of the ramdisk setting:

1. On Citrix XenServer, run the following command:
   ```
   xenstore-write /mh/limits/pv-ramdisk-max-size 536,870,912
   ```
2. Confirm the setting is in effect by running `xenstore-ls`.
   ```
   ----------------------
   limits = ""
   pv-kernel-max-size = "33554432"
   pv-ramdisk-max-size = "536,870,912"
   boot-time = ""
   ---------------------------
   ```
3. Remove the pending files left in `/run/xen/pygrub`.

The ramdisk setting returns to the default value after rebooting.

Multi-step firmware upgrades

Prior to using the FortiManager to push a multi-step firmware upgrade, confirm the upgrade path matches the path outlined on our support site. To confirm the path, please run:

```
dia fwmanager show-dev-upgrade-path <device name> <target firmware>
```

Alternatively, you can push one firmware step at a time.

Hyper-V FortiManager-VM running on an AMD CPU

A Hyper-V FMG-VM running on a PC with an AMD CPU may experience a kernel panic. Fortinet recommends running VMs on an Intel-based PC.

SSLv3 on FortiManager-VM64-AWS

Due to known vulnerabilities in the SSLv3 protocol, FortiManager-VM64-AWS only enables TLSv1 by default. All other models enable both TLSv1 and SSLv3. If you wish to disable SSLv3 support, please run:

```
config system global
set ssl-protocol t1sv1
```

```
    end
```

Upgrade Information

Prior to upgrading your FortiManager, please review the FortiManager Upgrade Guide in detail as it includes all of the necessary steps and associated details required to upgrade your FortiManager device or VM.

See FortiManager 7.2.2 Upgrade Guide.

You can upgrade FortiManager 7.0.1 or later directly to 7.2.2.

Before upgrading FortiManager, check ADOM versions. Check the ADOM versions supported by the destination firmware and the current firmware. If the current firmware uses ADOM versions not supported by the destination firmware, upgrade ADOM versions in FortiManager before upgrading FortiManager to the destination firmware version.

For example, FortiManager 7.0 supports ADOM versions 6.2, 6.4, and 7.0, but FortiManager 7.2 supports ADOM versions 6.4, 7.0, and 7.2. Before you upgrade FortiManager 7.0 to 7.2, ensure that all ADOM 6.2 versions have been upgraded to ADOM version 6.4 or later. See FortiManager 7.2.2 Upgrade Guide.

This section contains the following topics:

Downgrading to previous firmware versions

FortiManager does not provide a full downgrade path. You can downgrade to a previous firmware release by using the GUI or CLI, but doing so results in configuration loss. A system reset is required after the firmware downgrade process has completed. To reset the system, use the following CLI commands via a console port connection:

```
execute reset {all-settings | all-except-ip}
execute format {disk | disk-ext4 | disk-ext3}
```

Firmware image checksums

The MD5 checksums for all Fortinet software and firmware releases are available at the Customer Service & Support portal, https://support.fortinet.com. After logging in, go to *Download* > *Firmware Image Checksums*, enter the image file name including the extension, and select *Get Checksum Code*.

FortiManager VM firmware

Fortinet provides FortiManager VM firmware images for Amazon AWS, Amazon AWSOnDemand, Citrix and Open Source XenServer, Linux KVM, Microsoft Hyper-V Server, and VMware ESX/ESXi virtualization environments.

Amazon Web Services

- The 64-bit Amazon Machine Image (AMI) is available on the AWS marketplace.

Citrix XenServer and Open Source XenServer

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiManager VM installation.
- `.out.OpenXen.zip`: Download the 64-bit package for a new FortiManager VM installation. This package contains the QCOW2 file for the Open Source Xen Server.
- `.out.CitrixXen.zip`: Download the 64-bit package for a new FortiManager VM installation. This package contains the Citrix XenServer Virtual Appliance (XVA), Virtual Hard Disk (VHD), and OVF files.

Google Cloud Platform

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiManager VM installation.
- `.out.gcp.zip`: Download the 64-bit package for a new FortiManager VM installation.

Linux KVM

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiManager VM installation.
- `.out.kvm.zip`: Download the 64-bit package for a new FortiManager VM installation. This package contains QCOW2 that can be used by qemu.

Microsoft Azure

The files for Microsoft Azure have AZURE in the filenames, for example `<product>_VM64_AZURE-v<number>-build<number>-FORTINET.out.hyperv.zip`.

- `.out`: Download the firmware image to upgrade your existing FortiManager VM installation.

Microsoft Hyper-V Server

The files for Microsoft Hyper-V Server have HV in the filenames, for example, `<product>_VM64_HV-v<number>-build<number>-FORTINET.out.hyperv.zip`.

- `.out`: Download the firmware image to upgrade your existing FortiManager VM installation.
- `.hyperv.zip`: Download the package for a new FortiManager VM installation. This package contains a Virtual Hard Disk (VHD) file for Microsoft Hyper-V Server.

Microsoft Hyper-V 2016 is supported.

Oracle Private Cloud

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiManager VM installation.
- `.out.opc.zip`: Download the 64-bit package for a new FortiManager VM installation.

VMware ESX/ESXi

- `.out`: Download the 64-bit firmware image to upgrade your existing VM installation.
- `.ovf.zip`: Download either the 64-bit package for a new VM installation. This package contains an Open Virtualization Format (OVF) file for VMware and two Virtual Machine Disk Format (VMDK) files used by the OVF file during deployment.

For more information see the FortiManager Data Sheet available on the Fortinet web site. VM installation guides are available in the Fortinet Document Library.

SNMP MIB files

You can download the *FORTINET-FORTIMANAGER-FORTIANALYZER.mib* MIB file in the firmware image file folder. The Fortinet Core MIB file is located in the main FortiManager version 5.00 file folder.

Product Integration and Support

This section lists FortiManager 7.2.2 support of other Fortinet products. It also identifies what FortiManager features are supported for managed platforms and what languages FortiManager supports. It also lists which Fortinet models can be managed by FortiManager.

The section contains the following topics:

Supported software

FortiManager 7.2.2 supports the following software:

To confirm that a device model or firmware version is supported by the current firmware version running on FortiManager, run the following CLI command:

```
diagnose dvm supported-platforms list
```

Always review the Release Notes of the supported platform firmware version before upgrading your device.

Web browsers

FortiManager 7.2.2 supports the following web browsers:

- Microsoft Edge 80 (80.0.361 or later)
- Mozilla Firefox version 96
- Google Chrome version 97

Other web browsers may function correctly, but are not supported by Fortinet.

FortiOS and FortiOS Carrier

The *FortiManager Release Notes* communicate support for FortiOS versions that are available at the time of the FortiManager 7.2.2 release. For additional information about other supported FortiOS versions, please refer to the FortiManager compatibility chart in the Fortinet Document Library.

See FortiManager compatibility with FortiOS.

FortiManager 7.2.2 supports the following versions of FortiOS and FortiOS Carrier:

- 7.2.0 to 7.2.4
- 7.0.0 to 7.0.11
- 6.4.0 to 6.4.12

FortiADC

FortiManager 7.2.2 supports the following versions of FortiADC:

- 7.1.0 and later
- 7.0.0 and later
- 6.2.0 and later

FortiAnalyzer

FortiManager 7.2.2 supports the following versions of FortiAnalyzer:

- 7.2.0 and later
- 7.0.0 and later
- 6.4.0 and later

FortiAnalyzer-BigData

FortiManager 7.2.2 supports the following versions of FortiAnalyzer-BigData:

- 7.2.0 and later
- 7.0.0 and later

FortiAuthenticator

FortiManager 7.2.2 supports the following versions of FortiAuthenticator:

- 6.4.0 and later
- 6.3.0 and later
- 6.2.0 and later

FortiCache

FortiManager 7.2.2 supports the following versions of FortiCache:

- 4.2.0 and later
- 4.1.0 and later
- 4.0.0 and later

FortiClient

FortiManager 7.2.2 supports the following versions of FortiClient:

- 7.0.0 and later
- 6.4.0 and later
- 6.2.1 and later

FortiDDoS

FortiManager 7.2.2 supports the following versions of FortiDDoS:

- 6.4.0 and later
- 6.3.0 and later
- 6.2.0 and later

Limited support. For more information, see Feature support on page 24.

FortiDeceptor

FortiManager 7.2.2 supports the following versions of FortiDeceptor:

- 4.3.0 and later
- 4.2.0 and later

- 4.1.0 and later

FortiFirewall and FortiFirewallCarrier

FortiManager 7.2.2 supports the following versions of FortiFirewall and FortiFirewallCarrier:

- 7.2.0 and later
- 7.0.0 and later
- 6.4.0 and later

FortiMail

FortiManager 7.2.2 supports the following versions of FortiMail:

- 7.2.0 and later
- 7.0.0 and later
- 6.4.0 and later

FortiProxy

FortiManager 7.2.2 supports configuration management for the following versions of FortiProxy:

- 7.2.2
- 7.0.7

Configuration management support is identified as *Management Features* in these release notes. See Feature support on page 24.

FortiManager 7.2.2 supports logs from the following versions of FortiProxy:

- 7.2.0 to 7.2.4
- 7.0.0 to 7.0.9
- 2.0.0 to 2.0.5
- 1.2.0 to 1.2.13
- 1.1.0 to 1.1.6
- 1.0.0 to 1.0.7

FortiSandbox

FortiManager 7.2.2 supports the following versions of FortiSandbox:

- 4.2.0 and later
- 4.0.0 and 4.0.1
- 3.2.0 and later

FortiSOAR

FortiManager 7.2.2 supports the following versions of FortiSOAR:

- 7.3.0 and later
- 7.2.0 and later
- 7.0.0 and later

FortiSwitch ATCA

FortiManager 7.2.2 supports the following versions of FortiSwitch ATCA:

- 5.2.0 and later
- 5.0.0 and later
- 4.3.0 and later

FortiTester

FortiManager 7.2.2 supports the following versions of FortiTester:

- 7.1.0 and later
- 7.0.0 and later
- 4.2.0 and later

FortiWeb

FortiManager 7.2.2 supports the following versions of FortiWeb:

- 7.0.0 and later
- 6.4.0 and later
- 6.3.0 and later

Virtualization

FortiManager 7.2.2 supports the following virtualization software:

- Amazon Web Service AMI, Amazon EC2, Amazon EBS
- Citrix XenServer 7.2
- Google Cloud Platform
- Linux KVM Redhat 7.1
- Microsoft Azure
- Microsoft Hyper-V Server 2012, 2016, and 2019
- Nutanix AHV (AOS 5.10.5)
- OpenSource XenServer 4.2.5
- Oracle Private Cloud
- VMware ESXi versions 6.5 and later

Feature support

The following table lists FortiManager feature support for managed platforms.

Platform	Management Features	FortiGuard Update Services	VM License Activation	Reports	Logging
FortiGate	✓	✓	✓	✓	✓
FortiCarrier	✓	✓	✓	✓	✓
FortiADC		✓	✓		
FortiAnalyzer			✓	✓	✓
FortiAuthenticator					✓
FortiCache			✓	✓	✓
FortiClient		✓		✓	✓
FortiDDoS			✓	✓	✓
FortiDeceptor		✓			
FortiFirewall	✓				✓
FortiFirewall Carrier	✓				✓
FortiMail		✓	✓	✓	✓
FortiProxy	✓	✓	✓	✓	✓
FortiSandbox		✓	✓	✓	✓
FortiSOAR		✓	✓		
FortiSwitch ATCA	✓				
FortiTester		✓			
FortiWeb		✓	✓	✓	✓
Syslog					✓

Language support

The following table lists FortiManager language support information.

Language	GUI	Reports
English	✓	✓
Chinese (Simplified)	✓	✓

Language	GUI	Reports
Chinese (Traditional)	✓	✓
French	✓	✓
Japanese	✓	✓
Korean	✓	✓
Portuguese		✓
Spanish		✓

To change the FortiManager language setting, go to *System Settings* > *Admin* > *Admin Settings*, in *Administrative Settings* > *Language* select the desired language on the drop-down menu. The default value is *Auto Detect*.

Russian, Hebrew, and Hungarian are not included in the default report languages. You can create your own language translation files for these languages by exporting a predefined language from FortiManager, modifying the text to a different language, saving the file as a different language name, and then importing the file into FortiManager. For more information, see the *FortiManager Administration Guide*.

Supported models

The following tables list which FortiGate, FortiCarrier, FortiDDoS, FortiAnalyzer, FortiMail, FortiSandbox, FortiSwitch ATCA, FortiWeb, FortiCache, FortiProxy, and FortiAuthenticator models and firmware versions that can be managed by a FortiManager or send logs to a FortiManager running version 7.2.2.

Software license activated LENC devices are supported, if their platforms are in the supported models list. For example, support of FG-3200D indicates support of FG-3200D-LENC.

This section contains the following topics:

FortiGate models

The following FortiGate models are released with FortiOS firmware. For information about supported FortiGate models on special branch releases of FortiOS firmware, see FortiGate special branch models on page 28.

Model	Firmware Version
FortiGate: FortiGate-40F, FortiGate-40F-3G4G, FortiGate-60E, FortiGate-60E-DSL, FortiGate-60E-DSLJ, FortiGate-60E-POE, FortiGate-60F, FortiGate-61E, FortiGate-61F, FortiGate-80E, FortiGate-80E-POE, FortiGate-80F, FortiGate-80F-Bypass, FortiGate-80F-POE, FortiGate-81E, FortiGate-81E-POE, FortiGate-81F, FortiGate-81F-POE, FortiGate-90E, FortiGate-91E, FortiGate-100E, FortiGate-100EF, FortiGate-100F, FortiGate-101E, FortiGate-101F, FortiGate-140E, FortiGate-140E-POE, FortiGate-200E, FortiGate-200F, FortiGate-201E, FortiGate-201F, FortiGate-300E, FortiGate-301E, FortiGate-400E, FortiGate-400E-Bypass, FortiGate-401E, FortiGate-500E, FortiGate-501E, FortiGate-600E, FortiGate-601E, FortiGate-800D, FortiGate-900D, FortiGate-1000D, FortiGate-1100E, FortiGate-1101E, FortiGate-1500D, FortiGate-1500DT, FortiGate-1800F, FortiGate-1801F, FortiGate-2000E, FortiGate-2200E, FortiGate-2201E, FortiGate-2500E, FortiGate-2600F, FortiGate-2601F, FortiGate-3000D, FortiGate-3100D, FortiGate-3200D, FortiGate-3300E, FortiGate-3301E, FortiGate-3400E, FortiGate-3401E, FortiGate-3500F, FortiGate-3501F, FortiGate-3600E, FortiGate-3601E, FortiGate-3700D, FortiGate-3800D, FortiGate-3960E, FortiGate-3980E, FortiGate-4200F, FortiGate-4201F, FortiGate-4400F, FortiGate-4401F **FortiGate 5000 Series:** FortiGate-5001E, FortiGate-5001E1 **FortiGate DC:** FortiGate-401E-DC, FortiGate-800D-DC, FortiGate-1100E-DC, FortiGate-1500D-DC, FortiGate-1800F-DC, FortiGate-1801F-DC, FortiGate-2201E-ACDC, FortiGate-2600F-DC, FortiGate-2601F-DC, FortiGate-3000D-DC, FortiGate-3100D-DC, FortiGate-3200D-DC, FortiGate-3400E-DC, FortiGate-3401E-DC, FortiGate-3600E-DC, FortiGate-3700D-DC, FortiGate-3800D-DC, FortiGate-3960E-ACDC, FortiGate-3960E-DC, FortiGate-3980E-DC, FortiGate-4200F-DC, FortiGate-4201F-DC, FortiGate-4400F-DC, FortiGate-4401F-DC **FortiWiFi:** FWF-60E, FWF-60E-DSL, FWF-60E-DSLJ, FWF-60F, FWF-61E, FWF-61F, FWF-80F-2R, FWF-81F-2R, FWF-81F-2R-3G4G-POE, FWF-81F-2R-POE **FortiGate VM:** FortiGate-ARM64-AWS, FortiGate-ARM64-Azure, FortiGate-ARM64-GCP, FortiGate-ARM64-KVM, FortiGate-ARM64-OCI, FortiGate-VM64, FortiGate-VM64-ALI, FortiGate-VM64-AWS, FortiGate-VM64-Azure, FortiGate-VM64-GCP, FortiGate-VM64-HV, FortiGate-VM64-IBM, FortiGate-VM64-KVM, FortiGate-VM64-OPC, FortiGate-VM64-RAXONDEMAND, FortiGate-VM64-XEN, FortiGate-VMX-Service-Manager **FortiOS-VM:** FOS-VM64, FOS-VM64-HV, FOS-VM64-KVM, FOS-VM64-Xen **FortiGate Rugged:** FGR-60F, FGR-60F-3G4G	7.2

Model	Firmware Version
FortiGate: FortiGate-40F, FortiGate-40F-3G4G, FortiGate-60E, FortiGate-60E-DSL, FortiGate-60E-DSLJ, FortiGate-60E-POE, FortiGate-60F, FortiGate-61E, FortiGate-61F, FortiGate-80E, FortiGate-80E-POE, FortiGate-80F, FortiGate-80F-Bypass, FortiGate-80F-POE, FortiGate-81E, FortiGate-81E-POE, FortiGate-81F, FortiGate-81F-POE, FortiGate-90E, FortiGate-91E, FortiGate-100E, FortiGate-100EF, FortiGate-100F, FortiGate-101E, FortiGate-101F, FortiGate-140E, FortiGate-140E-POE, FortiGate-200E, FortiGate-200F, FortiGate-201E, FortiGate-201F, FortiGate-300D, FortiGate-300E, FortiGate-301E, FortiGate-400D, FortiGate-400E, FortiGate-400E-Bypass, FortiGate-401E, FortiGate-500D, FortiGate-500E, FortiGate-501E, FortiGate-600D, FortiGate-600E, FortiGate-601E, FortiGate-800D, FortiGate-900D, FortiGate-1000D, FortiGate-1100E, FortiGate-1101E, FortiGate-1200D, FortiGate-1500D, FortiGate-1500DT, FortiGate-1800F, FortiGate-1801F, FortiGate-2000E, FortiGate-2200E, FortiGate-2201E, FortiGate-2500E, FortiGate-2600F, FortiGate-2601F, FortiGate-3000D, FortiGate-3100D, FortiGate-3200D, FortiGate-3300E, FortiGate-3301E, FortiGate-3400E, FortiGate-3401E, FortiGate-3500F, FortiGate-3501F, FortiGate-3600E, FortiGate-3601E, FortiGate-3700D, FortiGate-3800D, FortiGate-3810D, FortiGate-3815D, FortiGate-3960E, FortiGate-3980E, FortiGate-4200F, FortiGate-4201F, FortiGate-4400F, FortiGate-4401F, **FortiGate 5000 Series:** FortiGate-5001D, FortiGate-5001E, FortiGate-5001E1 **FortiGate DC:** FortiGate-401E-DC, FortiGate-800D-DC, FortiGate-1100E-DC, FortiGate-1500D-DC, FortiGate-1800F-DC, FortiGate-1801F-DC, FortiGate-2201E-ACDC, FortiGate-2600F-DC, FortiGate-2601F-DC, FortiGate-3000D-DC, FortiGate-3100D-DC, FortiGate-3200D-DC, FortiGate-3400E-DC, FortiGate-3401E-DC, FortiGate-3600E-DC, FortiGate-3700D-DC, FortiGate-3800D-DC, FortiGate-3810D-DC, FortiGate-3815D-DC, FortiGate-3960E-ACDC, FortiGate-3960E-DC, FortiGate-3980E-DC, FortiGate-4200F-DC, FortiGate-4201F-DC, FortiGate-4400F-DC, FortiGate-4401F-DC **FortiWiFi:** FWF-60E, FWF-60E-DSL, FWF-60E-DSLJ, FWF-60F, FWF-61E, FWF-61F, FWF-80F-2R, FWF-81F-2R, FWF-81F-2R-3G4G-POE, FWF-81F-2R-POE **FortiGate VM:** FortiGate-ARM64-AWS, FortiGate-ARM64-KVM, FortiGate-ARM64-OCI, FortiGate-VM64, FortiGate-VM64-ALI, FortiGate-VM64-AWS, FortiGate-VM64-Azure, FortiGate-VM64-GCP, FortiGate-VM64-HV, FortiGate-VM64-IBM, FortiGate-VM64-KVM, FortiGate-VM64-OPC, FortiGate-VM64-RAXONDEMAND, FortiGate-VM64-XEN, FortiGate-VMX-Service-Manager **FortiOS-VM:** FOS-VM64, FOS-VM64-HV, FOS-VM64-KVM, FOS-VM64-Xen **FortiGate Rugged:** FGR-60F, FGR-60F-3G4G	7.0

Model	Firmware Version
FortiGate: FortiGate-40F, FortiGate-40F-3G4G, FortiGate-60E, FortiGate-60E-DSL, FortiGate-60E-DSLJ, FortiGate-60E-POE, FortiGate-60F, FortiGate-61E, FortiGate-61F, FortiGate-80E, FortiGate-80E-POE, FortiGate-80F, FortiGate-80F-Bypass, FortiGate-80F-POE, FortiGate-81E, FortiGate-81E-POE, FortiGate-81F, FortiGate-81F-POE, FortiGate-90E, FortiGate-91E, FortiGate-100D, FortiGate-100E, FortiGate-100EF, FortiGate-100F, FortiGate-101E, FortiGate-101F, FortiGate-140E, FortiGate-140E-POE, FortiGate-200E, FortiGate-200F, FortiGate-201E, FortiGate-201F, FortiGate-300D, FortiGate-300E, FortiGate-301E, FortiGate-400D, FortiGate-400E, FortiGate-400E-Bypass, FortiGate-401E, FortiGate-500D, FortiGate-500E, FortiGate-501E, FortiGate-600D, FortiGate-600E, FortiGate-601E, FortiGate-800D, FortiGate-900D, FortiGate-1000D, FortiGate-1100E, FortiGate-1101E, FortiGate-1200D, FortiGate-1500D, FortiGate-1500DT, FortiGate-1800F, FortiGate-1801F, FortiGate-2000E, FortiGate-2200E, FortiGate-2201E, FortiGate-2500E, FortiGate-2600F, FortiGate-2601F, FortiGate-3000D, FortiGate-3100D, FortiGate-3200D, FortiGate-3300E, FortiGate-3301E, FortiGate-3400E, FortiGate-3401E, FortiGate-3600E, FortiGate-3601E, FortiGate-3700D, FortiGate-3800D, FortiGate-3810D, FortiGate-3815D, FortiGate-3960E, FortiGate-3980E, FortiGate-4200F, FortiGate-4201F, FortiGate-4400F, FortiGate-4401F, **FortiGate 5000 Series:** FortiGate-5001D, FortiGate-5001E, FortiGate-5001E1 **FortiGate DC:** FortiGate-401E-DC, FortiGate-800D-DC, FortiGate-1100E-DC, FortiGate-1500D-DC, FortiGate-1800F-DC, FortiGate-1801F-DC, FortiGate-2201E-ACDC, FortiGate-2600F-DC, FortiGate-2601F-DC, FortiGate-3000D-DC, FortiGate-3100D-DC, FortiGate-3200D-DC, FortiGate-3400E-DC, FortiGate-3401E-DC, FortiGate-3600E-DC, FortiGate-3700D-DC, FortiGate-3800D-DC, FortiGate-3810D-DC, FortiGate-3815D-DC, FortiGate-3960E-ACDC, FortiGate-3960E-DC, FortiGate-3980E-DC, FortiGate-4200F-DC, FortiGate-4201F-DC, FortiGate-4400F-DC, FortiGate-4401F-DC **FortiGate Hardware Low Encryption:** FortiGate-100D-LENC **FortiWiFi:** FWF-40F, FWF-40F-3G4G, FWF-60E, FWF-60E-DSL, FWF-60E-DSLJ, FWF-60F, FWF-61E, FWF-61F, FWF-80F-2R, FWF-81F-2R, FWF-81F-2R-3G4G-POE, FWF-81F-2R-POE **FortiGate VM:** FortiGate-VM64, FortiGate-VM64-ALI, FortiGate-VM64-ALIONDEMAND, FortiGate-VM64-AWS, FortiGate-VM64-AZUREONDEMAND, FortiGate-VM64-Azure, FortiGate-VM64-GCP, VM64-GCPONDEMAND, FortiGate-VM64-HV, FortiGate-VM64-IBM, FortiGate-VM64-KVM, FortiGate-VM64-OPC, FortiGate-VM64-RAXONDEMAND, FortiGate-VM64-XEN, FortiGate-VMX-Service-Manager **FortiOS-VM:** FOS-VM64, FOS-VM64-HV, FOS-VM64-KVM, FOS-VM64-Xen **FortiGate Rugged:** FGR-60F, FGR-60F-3G4G	6.4

FortiGate special branch models

The following FortiGate models are released on special branches of FortiOS. FortiManager version 7.2.2 supports these models on the identified FortiOS version and build number.

For information about supported FortiGate models released with FortiOS firmware, see FortiGate models on page 26.

FortiOS 7.0

FortiGate Model	FortiOS Version	FortiOS Build
FortiGate-70F, FortiGate-71F	7.0.8	4682
FortiGate-80F-DSL	7.0.7	4730
FortiGate-400F, FortiGate-401F	7.0.9	4777
FortiGate-600F, FortiGate-601F	7.0.9	4777
FortiGate-1000F, FortiGate-1001F	7.0.9	6423
FortiGate-1500G, FortiGate-1501G	7.0.9	6458
FortiGate-3000F, FortiGate-3001F	7.0.9	4777
FortiGate-3200F	7.0.7	6405
FortiGate-3201F	7.0.7	6369
FortiGate-3700F, FortiGate-3701F	7.0.6	6118
FortiGate-4800F, FortiGate-4801F	7.0.7	6401
FortiGate-6000F, FortiGate-6300F, FortiGate-6300F-DC, FortiGate-6301F, FortiGate-6301F-DC, FortiGate-6500F, FortiGate-6500F-DC, FortiGate-6501F, FortiGate-6501F-DC	7.0.5	29
FortiGate-7000E, FortiGate-7030E, FortiGate-7040E, FortiGate-7060E, FortiGate-7060E-8-DC FortiGate-7000F, FortiGate-7081F, FortiGate-7121F, FortiGate-7121F-2, FortiGate-7121F-2-DC, FortiGate-7121F-DC	7.0.5	29
FortiGateRugged-70F	7.0.6	6318
FortiGateRugged-70F-3G4G	7.0.6	6283

FortiOS 6.4

FortiGate Model	FortiOS Version	FortiOS Build
FortiGate-400F, FortiGate-401F	6.4.8	5206
FortiGate-600F	6.4.8	5306
FortiGate-601F	6.4.8	5301
FortiGate-3500F	6.4.6	5886
FortiGate-3501F	6.4.6	6132

FortiGate Model	FortiOS Version	FortiOS Build
FortiGate-6000F, FortiGate-6300F, FortiGate-6300F-DC, FortiGate-6301F, FortiGate-6301F-DC, FortiGate-6500F, FortiGate-6500F-DC, FortiGate-6501F, FortiGate-6501F-DC	6.4.10	1875
FortiGate-7000E, FortiGate-7030E, FortiGate-7040E, FortiGate-7060E, FortiGate-7060E-8-DC FortiGate-7000F, FortiGate-7081F, FortiGate-7121F, FortiGate-7121F-2, FortiGate-7121F-2-DC, FortiGate-7121F-DC	6.4.10	1875
FortiWiFi-80F-2R-3G4G-DSL	6.4.7	5003

FortiCarrier models

The following FortiCarrier models are released with FortiCarrier firmware.

For information about supported FortiCarrier models on special branch releases of FortiCarrier firmware, see FortiCarrier special branch models on page 31.

Model	Firmware Version
FortiCarrier: FortiCarrier-3000D, FortiCarrier-3100D, FortiCarrier-3200D, FortiCarrier-3300E, FortiCarrier-3301E, FortiCarrier-3400E, FortiCarrier-3401E, FortiCarrier-3500F, FortiCarrier-3501F, FortiCarrier-3600E, FortiCarrier-3601E, FortiCarrier-3700D, FortiCarrier-3800D, FortiCarrier-3960E, FortiCarrier-3980E, FortiCarrier-4200F, FortiCarrier-4201F, FortiCarrier-4400F, FortiCarrier-4401F, FortiCarrier-5001E, FortiCarrier-5001E1 **FortiCarrier-DC**: FortiCarrier-3000D-DC, FortiCarrier-3100D-DC, FortiCarrier-3200D-DC, FortiCarrier-3400E-DC, FortiCarrier-3401E-DC, FortiCarrier-3600E-DC, FortiCarrier-3700D-DC, FortiCarrier-3800D-DC, FortiCarrier-3960E-DC, FortiCarrier-3980E-DC, FortiCarrier-4200F-DC, FortiCarrier-4201F-DC, FortiCarrier-4400F-DC, FortiCarrier-4401F-DC **FortiCarrier-VM**: FortiCarrier-ARM64-AWS, FortiCarrier-ARM64-GCP, FortiCarrier-ARM64-KVM, FortiCarrier-ARM64-OCI, FortiCarrier-VM64, FortiCarrier-VM64-ALI, FortiCarrier-VM64-AWS, FortiCarrier-VM64-Azure, FortiCarrier-VM64-GCP, FortiCarrier-VM64-HV, FortiCarrier-VM64-IBM, FortiCarrier-VM64-KVM, FortiCarrier-VM64-OPC, FortiCarrier-VM64-Xen	7.2
FortiCarrier: FortiCarrier-3000D, FortiCarrier-3100D, FortiCarrier-3200D, FortiCarrier-3300E, FortiCarrier-3301E, FortiCarrier-3400E, FortiCarrier-3401E, FortiCarrier-3500F, FortiCarrier-3501F, FortiCarrier-3600E, FortiCarrier-3601E, FortiCarrier-3700D, FortiCarrier-3800D, FortiCarrier-3810D, FortiCarrier-3815D, FortiCarrier-3960E, FortiCarrier-3980E, FortiCarrier-5001D, FortiCarrier-5001E, FortiCarrier-5001E1 **FortiCarrier-DC**: FortiCarrier-3000D-DC, FortiCarrier-3100D-DC, FortiCarrier-3200D-DC, FortiCarrier-3400E-DC, FortiCarrier-3401E-DC, FortiCarrier-3600E-DC, FortiCarrier-3700D-DC, FortiCarrier-3800D-DC, FortiCarrier-3810D-DC, FortiCarrier-3815D-DC, FortiCarrier-3960E-DC, FortiCarrier-3980E-DC	7.0

Model	Firmware Version
FortiCarrier-VM: FortiCarrier-ARM64-AWS, FortiCarrier-ARM64-KVM, FortiCarrier-ARM64-OCI, FortiCarrier-VM64, FortiCarrier-VM64-ALI, FortiCarrier-VM64-AWS, FortiCarrier-VM64-Azure, FortiCarrier-VM64-GCP, FortiCarrier-VM64-HV, FortiCarrier-VM64-IBM, FortiCarrier-VM64-KVM, FortiCarrier-VM64-OPC, FortiCarrier-VM64-Xen, FortiCarrier-ARM64-KVM	
FortiCarrier: FortiCarrier-3000D, FortiCarrier-3100D, FortiCarrier-3200D, FortiCarrier-3300E, FortiCarrier-3301E, FortiCarrier-3400E, FortiCarrier-3401E, FortiCarrier-3500F, FortiCarrier-3501F, FortiCarrier-3600E, FortiCarrier-3601E, FortiCarrier-3700D, FortiCarrier-3800D, FortiCarrier-3810D, FortiCarrier-3815D, FortiCarrier-3960E, FortiCarrier-3980E, FortiCarrier-5001D, FortiCarrier-5001E, FortiCarrier-5001E1 **FortiCarrier-DC:** FortiCarrier-3000D-DC, FortiCarrier-3100D-DC, FortiCarrier-3200D-DC, FortiCarrier-3400E-DC, FortiCarrier-3401E-DC, FortiCarrier-3600E-DC, FortiCarrier-3700D-DC, FortiCarrier-3800D-DC, FortiCarrier-3810D-DC, FortiCarrier-3815D-DC, FortiCarrier-3960E-DC, FortiCarrier-3980E-DC **FortiCarrier-VM:** FortiCarrier-VM64, FortiCarrier-VM64-ALI, FortiCarrier-VM64-AWS, FortiCarrier-VM64-Azure, FortiCarrier-VM64-GCP, FortiCarrier-VM64-HV, FortiCarrier-VM64-IBM, FortiCarrier-VM64-KVM, FortiCarrier-VM64-OPC, FortiCarrier-VM64-Xen	6.4

FortiCarrier special branch models

The following FortiCarrier models are released on special branches of FortiOS Carrier. FortiManager version 7.2.2 supports these models on the identified FortiOS Carrier version and build number.

For information about supported FortiCarrier models released with FortiOS Carrier firmware, see FortiCarrier models on page 30.

FortiCarrier 7.0

FortiCarrier Model	FortiCarrier Version	FortiCarrier Build
FortiCarrier-3000F, FortiCarrier-3001F	7.0.9	4777
FortiCarrier-3200F	7.0.7	6405
FortiCarrier-3201F	7.0.7	6369
FortiCarrier-3700F, FortiCarrier-3701F	7.0.6	6118
FortiCarrier-4800F, FortiCarrier-4801F	7.0.7	6401
FortiCarrier-6000F, FortiCarrier-6300F, FortiCarrier-6300F-DC, FortiCarrier-6301F, FortiCarrier-6301F-DC, FortiCarrier-6500F, FortiCarrier-6500F-DC, FortiCarrier-65001F, FortiCarrier-6501F-DC	7.0.5	29
FortiCarrier-7000E, FortiCarrier-7030E, FortiCarrier-7040E, FortiCarrier-7060E, FortiCarrier-7060E-8-DC	7.0.5	29

FortiCarrier Model	FortiCarrier Version	FortiCarrier Build
FortiCarrier-7000F, FortiCarrier-7081F, FortiCarrier-7121F, FortiCarrier-7121F-2, FortiCarrier-7121F-2-DC, FortiCarrier-7121F-DC		

FortiCarrier 6.4

FortiCarrier Model	FortiCarrier Version	FortiCarrier Build
FortiCarrier-3500F	6.4.6	5886
FortiCarrier-3501F	6.4.6	6132
FortiCarrier-6000F, FortiCarrier-6300F, FortiCarrier-6300F-DC, FortiCarrier-6301F, FortiCarrier-6301F-DC, FortiCarrier-6500F, FortiCarrier-6500F-DC, FortiCarrier-65001F, FortiCarrier-6501F-DC	6.4.10	1875
FortiCarrier-7000E, FortiCarrier-7030E, FortiCarrier-7040E, FortiCarrier-7060E, FortiCarrier-7060E-8-DC FortiCarrier-7000F, FortiCarrier-7081F, FortiCarrier-7121F, FortiCarrier-7121F-2, FortiCarrier-7121F-2-DC, FortiCarrier-7121F-DC	6.4.10	1875

FortiADC models

Model	Firmware Version
FortiADC: FortiADC-100F, FortiADC-120F, FortiADC-200D, FortiADC-200F, FortiADC-220F, FortiADC-300D, FortiADC-300F, FortiADC-400D, FortiADC-400F, FortiADC-700D, FortiADC-1000F, FortiADC-1200F, FortiADC-1500D, FortiADC-2000D, FortiADC-2000F, FortiADC-2200F, FortiADC-4000D, FortiADC-4000F, FortiADC-4200F, FortiADC-5000F **FortiADC VM**: FortiADC-VM	7.1
FortiADC: FortiADC-100F, FortiADC-120F, FortiADC-200D, FortiADC-200F, FortiADC-220F, FortiADC-300D, FortiADC-300F, FortiADC-400D, FortiADC-400F, FortiADC-700D, FortiADC-1000F, FortiADC-1200F, FortiADC-1500D, FortiADC-2000D, FortiADC-2000F, FortiADC-2200F, FortiADC-4000D, FortiADC-4000F, FortiADC-4200F, FortiADC-5000F **FortiADC VM**: FortiADC-VM	7.0
FortiADC: FortiADC-100F, FortiADC-120F, FortiADC-200D, FortiADC-200F, FortiADC-220F, FortiADC-300D, FortiADC-300F, FortiADC-400D, FortiADC-400F, FortiADC-700D, FortiADC-1000F, FortiADC-1200F, FortiADC-1500D, FortiADC-2000D, FortiADC-2000F, FortiADC-2200F, FortiADC-4000D, FortiADC-4000F, FortiADC-4200F, FortiADC-5000F **FortiADC VM**: FortiADC-VM	6.2

FortiAnalyzer models

Model	Firmware Version
FortiAnalyzer: FortiAnalyzer-150G, FortiAnalyzer-300F, FortiAnalyzer-300G, FortiAnalyzer-400E, FortiAnalyzer-800F, FortiAnalyzer-800G, FortiAnalyzer-1000F, FortiAnalyzer-2000E, FortiAnalyzer-3000E, FortiAnalyzer-3000F, FortiAnalyzer-3000G, FortiAnalyzer-3500E, FortiAnalyzer-3500F, FortiAnalyzer-3500G, FortiAnalyzer-3700F, FortiAnalyzer-3700G, FortiAnalyzer-3900E **FortiAnalyzer VM**: FortiAnalyzer-DOCKER, FortiAnalyzer-VM64, FortiAnalyzer-VM64-ALI, FortiAnalyzer-VM64-AWS, FortiAnalyzer-VM64-AWS-OnDemand, FortiAnalyzer-VM64-Azure, FortiAnalyzer-VM64-Azure-OnDemand, FortiAnalyzer-VM64-GCP, FortiAnalyzer-VM64-HV, FortiAnalyzer-VM64-IBM, FortiAnalyzer-VM64-KVM, FortiAnalyzer-VM64-OPC, FortiAnalyzer-VM64-Xen	7.2
FortiAnalyzer: FortiAnalyzer-150G, FortiAnalyzer-200F, FortiAnalyzer-300F, FortiAnalyzer-300G, FortiAnalyzer-400E, FortiAnalyzer-800F, FortiAnalyzer-800G, FortiAnalyzer-1000F, FortiAnalyzer-2000E, FortiAnalyzer-3000E, FortiAnalyzer-3000F, FortiAnalyzer-3000G, FortiAnalyzer-3500E, FortiAnalyzer-3500F, FortiAnalyzer-3500G, FortiAnalyzer-3700F, FortiAnalyzer-3700G, FortiAnalyzer-3900E **FortiAnalyzer VM**: FortiAnalyzer-DOCKER, FortiAnalyzer-VM64, FortiAnalyzer-VM64-ALI, FortiAnalyzer-VM64-ALI-OnDemand, FortiAnalyzer-VM64-AWS, FortiAnalyzer-VM64-Azure, FortiAnalyzer-VM64-Azure-OnDemand, FortiAnalyzer-VM64-GCP, FortiAnalyzer-VM64-GCP-OnDemand, FortiAnalyzer-VM64-HV, FortiAnalyzer-VM64-IBM, FortiAnalyzer-VM64-KVM, FortiAnalyzer-VM64-OPC, FortiAnalyzer-VM64-Xen	7.0
FortiAnalyzer: FortiAnalyzer-150G, FortiAnalyzer-200F, FortiAnalyzer-300F, FortiAnalyzer-300G, FortiAnalyzer-400E, FortiAnalyzer-800F, FortiAnalyzer-800G, FortiAnalyzer-1000E, FortiAnalyzer-1000F, FortiAnalyzer-2000E, FortiAnalyzer-3000E, FortiAnalyzer-3000F, FortiAnalyzer-3000G, FortiAnalyzer-3500E, FortiAnalyzer-3500F, FortiAnalyzer-3500G, FortiAnalyzer-3700F, FortiAnalyzer-3700G, FortiAnalyzer-3900E **FortiAnalyzer VM:** FortiAnalyzer-DOCKER, FortiAnalyzer-VM64, FortiAnalyzer-VM64-ALI, FortiAnalyzer-VM64-ALI-OnDemand, FortiAnalyzer-VM64-AWS, FortiAnalyzer-VM64-AWSOnDemand, FortiAnalyzer-VM64-Azure, FortiAnalyzer-VM64-Azure-OnDemand, FortiAnalyzer-VM64-GCP, FortiAnalyzer-VM64-GCP-OnDemand, FortiAnalyzer-VM64-HV, FortiAnalyzer-VM64-KVM, FortiAnalyzer-VM64-OPC, FortiAnalyzer-VM64-Xen	6.4

FortiAnalyzer-BigData models

Model	Firmware Version
FortiAnalyzer-BigData: FortiAnalyzer-BigData-4500F **FortiAnalyzer-BigData VM**: FortiAnalyzer-BigData-VM64	7.2
FortiAnalyzer-BigData: FortiAnalyzer-BigData-4500F **FortiAnalyzer-BigData VM**: FortiAnalyzer-BigData-VM64	7.0

FortiAuthenticator models

Model	Firmware Version
FortiAuthenticator: FAC-200D, FAC-200E, FAC-300F, FAC-400C, FAC-400E, FAC-800F, FAC-1000C, FAC-1000D, FAC-2000E, FAC-3000D, FAC-3000E, FAC-3000F **FortiAuthenticator VM:** FAC-VM	6.4
FortiAuthenticator: FAC-200D, FAC-200E, FAC-300F, FAC-400C, FAC-400E, FAC-800F, FAC-1000C, FAC-1000D, FAC-2000E, FAC-3000D, FAC-3000E **FortiAuthenticator VM:** FAC-VM	6.2, 6,3

FortiCache models

Model	Firmware Version
FortiCache: FCH-400C, FCH-400E, FCH-1000C, FCH-1000D, FCH-3000C, FCH-3000D, FCH-3000E, FCH-3900E **FortiCache VM:** FCH-KVM, FCH-VM64	4.1, 4.2
FortiCache: FCH-400C, FCH-400E, FCH-1000C, FCH-1000D, FCH-3000C, FCH-3000D, FCH-3900E **FortiCache VM:** FCH-VM64	4.0

FortiDDoS models

Model	Firmware Version
FortiDDoS: FortiDDoS-200F, FortiDDoS-1500F, FortiDDoS-2000F, FortiDDoS-3000F **FortiDDoS VM**: FortiDDoS-VM	6.4
FortiDDoS: FortiDDoS-200F, FortiDDoS-1500F, FortiDDoS-2000F **FortiDDoS VM**: FortiDDoS-VM	6.3
FortiDDoS: FortiDDoS-200F, FortiDDoS-1500F **FortiDDoS VM**: FortiDDoS-VM	6.2

FortiDeceptor models

Model	Firmware Version
FortiDeceptor: FDC-1000F, FDC-1000G **FortiDeceptor Rugged**: FDCR-100G **FortiDeceptor VM**: FDC-VM	4.3
FortiDeceptor: FDC-1000F, FDC-1000G	4.2

Model	Firmware Version
FortiDeceptor Rugged: FDCR-100G **FortiDeceptor VM**: FDC-VM	
FortiDeceptor: FDC-1000F, FDC-1000G **FortiDeceptor Rugged**: FDCR-100G **FortiDeceptor VM**: FDC-VM	4.1

FortiFirewall models

Some of the following FortiFirewall models are released on special branches of FortiFirewall firmware. FortiManager version 7.2.2 supports these models on the identified FortiFirewall firmware version and build number.

Model	Firmware Version	Firmware Build
FortiFirewall: FortiFirewall-1801F **FortiFirewall DC**: FortiFirewall-1801F-DC	6.4.9	5334
FortiFirewall: FortiFirewall-2600F **FortiFirewall DC**: FortiFirewall-2600F-DC	6.4.9	5305
FortiFirewall: FortiFirewall-3980E **FortiFirewall DC**: FortiFirewall-3980E-DC	6.2	1262
FortiFirewall: FortiFirewall-3980E **FortiFirewall DC**: FortiFirewall-3980E-DC	6.4	2020
FortiFirewall: FortiFirewall-4200F	6.2.7	5141
FortiFirewall: FortiFirewall-4200F, FortiFirewall-4400F	6.4	1999
FortiFirewall: FortiFirewall-4400F	6.2.7	5148
FortiFirewall: FortiFirewall-4401F **FortiFirewall DC**: FortiFirewall-4401F-DC	6.4.9	5318
FortiFirewall-VM: FortiFirewall-VM64, FortiFirewall-VM64-KVM	6.4	1999
FortiFirewall-VM: FortiFirewall-VM64, FortiFirewall-VM64-KVM	7.2	1384

FortiFirewallCarrier models

Some of the following FortiFirewallCarrier models are released on special branches of FortiFirewallCarrier firmware. FortiManager version 7.2.2 supports these models on the identified FortiFirewallCarrier firmware version and build number.

Model	Firmware Version	Firmware Build
FortiFirewallCarrier: FortiFirewallCarrier-4200F, FortiFirewallCarrier-4400F	6.4	1999
FortiFirewallCarrier: FortiFirewallCarrier-4200F, FortiFirewallCarrier-4400F	6.2.7	5148
FortiFirewallCarrier: FortiFirewallCarrier-4401F	6.4.9	5318

FortiMail models

Model	Firmware Version
FortiMail: FE-60D, FE-200D, FE-200E, FE-200F, FE-400E, FE-400F, FE-900F, FE-2000F, FE-3000F	7.2
FortiMail: FE-60D, FE-200D, FE-200E, FE-200F, FE-400E, FE-400F, FE-900F, FE-1000D, FE-2000E, FE-2000F, FE-3000D, FE-3000E, FE-3000F, FE-3200E **FortiMail VM:** FML-VM	7.0
FortiMail: FE-60D, FE-200D, FE-200E, FE-200F, FE-400E, FE-400F, FE-900F, FE-1000D, FE-2000E, FE-3000D, FE-3000E, FE-3200E **FortiMail VM:** FML-VM	6.4

FortiProxy models

Model	Firmware Version
FortiProxy: FPX-400E, FPX-2000E, FPX-4000E, **FortiProxy VM:** FortiProxy-AliCloud, FortiProxy-AWS, FortiProxy-Azure, FortiProxy-GCP, FortiProxy-HyperV, FortiProxy-KVM, FortiProxy-VM64	7.2
FortiProxy: FPX-400E, FPX-400G, FPX-2000E, FPX-2000G, FPX-4000E, FPX-4000G **FortiProxy VM:** FortiProxy-AliCloud, FortiProxy-AWS, FortiProxy-Azure, FortiProxy-GCP, FortiProxy-HyperV, FortiProxy-KVM, FortiProxy-VM64	7.0
FortiProxy: FPX-400E, FPX-2000E, FPX-4000E **FortiProxy VM:** FortiProxy-KVM, FortiProxy-VM64	1.0, 1.1, 1.2, 2.0

FortiSandbox models

Model	Firmware Version
FortiSandbox: FSA-500F, FSA-1000D, FSA-1000F, FSA-2000E, FSA-3000D, FSA-3000E, FSA-3000F, FSA-3500D **FortiSandbox DC:** FSA-1000F-DC	4.2

Model	Firmware Version
FortiSandbox-VM: FortiSandbox-AWS, FortiSandbox-Cloud, FSA-VM	
FortiSandbox: FSA-500F, FSA-1000D, FSA-1000F, FSA-2000E, FSA-3000D, FSA-3000E, FSA-3000F, FSA-3500D **FortiSandbox DC:** FSA-1000F-DC **FortiSandbox-VM:** FortiSandbox-AWS, FortiSandbox-Cloud, FSA-VM	4.0
FortiSandbox: FSA-500F, FSA-1000D, FSA-1000F, FSA-2000E, FSA-3000D, FSA-3000E, FSA-3500D **FortiSandbox DC:** FSA-1000F-DC **FortiSandbox-VM:** FortiSandbox-AWS, FSA-VM	3.2

FortiSOAR models

Model	Firmware Version
FortiSOAR VM: FortiSOAR-VM	7.0, 7.2, 7.3

FortiSwitch ATCA models

Model	Firmware Version
FortiController: FTCL-5103B, FTCL-5903C, FTCL-5913C	5.2
FortiSwitch-ATCA: FS-5003A, FS-5003B **FortiController:** FTCL-5103B	5.0
FortiSwitch-ATCA: FS-5003A, FS-5003B	4.3

FortiTester models

Model	Firmware Version
FortiTester: FortiTester-60F, FortiTester-100F, FortiTester-2000D, FortiTester-2000E, FortiTester-2000F, FortiTester-2500E, FortiTester-3000E, FortiTester-3000F, FortiTester-4000E, FortiTester-4000F **FortiTester VM:** FortiTester-VM, FortiTester-VM-ALI-BYOL, FortiTester-VM-ALI-PAYG, FortiTester-VM-AWS-BYOL, FortiTester-VM-AWS-PAYG, FortiTester-VM-AZURE-BYOL, FortiTester-VM-AZURE-PAYG, FortiTester-VM-GCP-BYOL, FortiTester-VM-GCP-PAYG, FortiTester-VM-IBM-PAYG, FortiTester-VM-KVM, FortiTester-VM-OCI-BYOL, FortiTester-VM-OCI-PAYG	7.1
FortiTester: FortiTester-60F, FortiTester-100F, FortiTester-2000D, FortiTester-2000E, FortiTester-2000F, FortiTester-2500E, FortiTester-3000E, FortiTester-3000F, FortiTester-4000E, FortiTester-4000F	7.0

Model	Firmware Version
FortiTester VM: FortiTester-VM, FortiTester-VM-ALI-BYOL, FortiTester-VM-ALI-PAYG, FortiTester-VM-AWS-BYOL, FortiTester-VM-AWS-PAYG, FortiTester-VM-AZURE-BYOL, FortiTester-VM-AZURE-PAYG, FortiTester-VM-GCP-BYOL, FortiTester-VM-GCP-PAYG, FortiTester-VM-IBM-PAYG, FortiTester-VM-KVM, FortiTester-VM-OCI-BYOL, FortiTester-VM-OCI-PAYG	
FortiTester: FortiTester-60F, FortiTester-100F, FortiTester-2000D, FortiTester-2000E, FortiTester-2500E, FortiTester-3000E, FortiTester-3000F, FortiTester-4000E, FortiTester-4000F **FortiTester VM:** FortiTester-VM, FortiTester-VM-ALI-BYOL, FortiTester-VM-ALI-PAYG, FortiTester-VM-AWS-BYOL, FortiTester-VM-AWS-PAYG, FortiTester-VM-AZURE-BYOL, FortiTester-VM-AZURE-PAYG, FortiTester-VM-GCP-BYOL, FortiTester-VM-GCP-PAYG, FortiTester-VM-KVM, FortiTester-VM-OCI-BYOL, FortiTester-VM-OCI-PAYG	4.2

FortiWeb models

Model	Firmware Version
FortiWeb: FortiWeb-100D, FortiWeb-100E, FortiWeb-400C, FortiWeb-400D, FortiWeb-400E, FortiWeb-600D, FortiWeb-600E, FortiWeb-1000D, FortiWeb-1000E, FortiWeb-2000E, FortiWeb-2000F, FortiWeb-3000C, FortiWeb-3000CFSX, FortiWeb-3000D, FortiWeb-3000DFSX, FortiWeb-3000E, FortiWeb-3000F, FortiWeb-3010E, FortiWeb-4000C, FortiWeb-4000D, FortiWeb-4000E, FortiWeb-4000F **FortiWeb VM:** FortiWeb-Azure, FortiWeb-Azure_OnDemand, FortiWeb-Docker, FortiWeb-GCP, FortiWeb-GCP_OnDemand, FortiWeb-HyperV, FortiWeb-VM, FortiWeb-XENOpenSource, FortiWeb-XENServer	6.4, 7.0
FortiWeb: FortiWeb-100D, FortiWeb-100E, FortiWeb-400C, FortiWeb-400D, FortiWeb-400E, FortiWeb-600D, FortiWeb-600E, FortiWeb-1000D, FortiWeb-1000E, FortiWeb-2000E, FortiWeb-3000C, FortiWeb-3000CFSX, FortiWeb-3000D, FortiWeb-3000DFSX, FortiWeb-3000E, FortiWeb-3010E, FortiWeb-4000C, FortiWeb-4000D, FortiWeb-4000E **FortiWeb VM:** FortiWeb-Azure, FortiWeb-Azure_OnDemand, FortiWeb-Docker, FortiWeb-GCP, FortiWeb-GCP_OnDemand, FortiWeb-HyperV, FortiWeb-VM, FortiWeb-XENOpenSource, FortiWeb-XENServer	6.3

Compatibility with FortiOS Versions

This section highlights compatibility issues that administrators should be aware of in FortiManager 7.2.2.

FortiManager 7.2.2 and FortiOS 6.4.12 compatibility issues

This section identifies interoperability issues that have been identified with FortiManager 7.2.2 and FortiOS 6.4.12. FortiOS 6.4.12 includes syntax changes not supported by FortiManager 7.2.2.

The following objects were removed:

- (attr) system global http-request-limit
- (attr) system global http-unauthenticated-request-limit

FortiManager 7.2.2 and FortiOS 7.0.10 compatibility issues

This section identifies interoperability issues that have been identified with FortiManager 7.2.2 and FortiOS 7.0.10. FortiOS 7.0.10 includes syntax changes not supported by FortiManager 7.2.2.

The following objects were removed:

- (attr) system global http-request-limit
- (attr) system global http-unauthenticated-request-limit

FortiManager 7.2.2 and FortiOS 7.0.11 compatibility issues

This section identifies interoperability issues that have been identified with FortiManager 7.2.2 and FortiOS 7.0.11. FortiOS 7.0.11 includes syntax changes not supported by FortiManager 7.2.2.

When specific platforms are indicated, the syntax change applies to both the FortiGate and FortiCarrier platform for the model.

For example, `(4 platforms: 3980E,3960E)` indicates FortiGate-3980E, FortiCarrier-3980E, FortiGate-3960E, FortiCarrier-3960E.

The following objects were added:

- `(attr) endpoint-control fctems ca-cn-info`
- `(attr) endpoint-control fctems trust-ca-cn`
- `(node) system replacemsg custom-message`

The following default values changed:

- `system interface mediatype` default value changed from `none` to `qsfp28-sr4`
- `system lte-modem auto-connect` default value changed from `disable` to `enable`
- `system lte-modem gps-service` default value changed from `disable` to `enable`
- `system npu hash-config` default value is changed depending on the platform. For more information, see the FortiOS Hardware Acceleration Guide on the Fortinet Documents Library.

Additional option changes:

```
system interface mediatype
   option-list (tag|opt): ["cr", "cr4", "gmii", "lr", "lr4", "none", "sgmii", "sr",
        "sr4"] -> None (4 platforms: 3980E,3960E)
   option-list (tag|opt): None -> ["qsfp28-cr4", "qsfp28-lr4", "qsfp28-sr4"] (4
        platforms: 3980E,3960E)
system interface speed
   option-list (tag|opt): None -> ["2500auto", "5000auto"] (36 platforms:
        2200E,3301E,3980E,2601F,3501F,4200F,3500F,1800F,3600E,1100E,4401F,2201E,1801F,330
        0E,3400E,2600F,4201F,3601E,1101E,3960E,3401E,4400F)
system link-monitor interval
   int-range (tag|lmt): 500,3600000 -> 20,3600000
system link-monitor probe-timeout
   int-range (tag|lmt): 500,5000 -> 20,200
system sdwan health-check interval
   int-range (tag|lmt): 500,3600000 -> 20,3600000
system sdwan health-check probe-timeout
   int-range (tag|lmt): 500,3600000 -> 20,3600000
webfilter profile
   tab-size (tag|tz): 20000,20000,0 -> 35000,35000,0 (16 platforms:
        4200F,4401F,4201F,3601E,3980E,3600E,3960E,4400F)
webfilter urlfilter
   tab-size (tag|tz): 1000,1000,0 -> 35000,35000,0 (16 platforms:
        4200F,4401F,4201F,3601E,3980E,3600E,3960E,4400F)
```

Resolved Issues

The following issues have been fixed in 7.2.2. To inquire about a particular bug, please contact Customer Service & Support.

AP Manager

Bug ID	Description
661938	FortiManager displays an error when trying to edit and save managed APs.
819137	Installation failed if Distributed Automatic Radio Resource Provisioning (DARRP) is disabled on AP Profile.
822525	FortiManager does not take the per-device mapping authentication config for SSID under the WiFi Profiles.
824032	Some of the FAPs Radio configuration settings under the AP's profile are missing.
853345	The clients are connected to the Wireless Access Point, however, "clients" section under the diagnostics & tools of AP does not display any info.
861579	Unable to add the AP to the *AP Manager* due to the error "Parent object does not exist" message.

Device Manager

Bug ID	Description
472443	FortiManager does not retrieve any of the profiles and addresses in the format of "g-XXX" from FortiGates when VDOMs are enabled.
657988	FortiManager may lose connection and fail to install after FortiGate HA switching roll.
723006	FortiManager does not support creating the "DHCP Reservation" under the "Network Monitors Widget".
738276	FortiManager's GUI does not display the "Routing Objects" under "Router".
745122	FortiManager unsets the ipv6 configuration during the installation to the FortiGate.
745586	Local firmware images are duplicated under the *Device Manager*.
748579	CLI configurations for SD WAN template is not working properly.
761066	FortiManager does not display the VLAN's protocols on GUI for FortiGates.

Bug ID	Description
763036	Physical Interface Members are not displayed for the "Hardware Switch" type on FortiManager when FortiGates are added using Model Device method to the FortiManager.
773338	Unable to save the Virtual Router Redundancy Protocol (VRRP) settings for FortiGate's interfaces.
786264	Unable to delete default "wireless-controller" "vap" configuration from the device DB.
788923	SD-WAN template does not change the value of "service-sla-tie-break" for a SDWAN Zone.
789249	FortiManager does not have Logging Options after enabling One-Arm Sniffer under Interface.
789544	Status of the "Firmware Template" has been changed to "Unknown" after upgrade.
794764	FortiGate Modem Interface is not visible under *Device Manager*.
797404	After successfully running all the Assigned Templates to FortiGates, the status is displayed as *Modified*.
800191	During the ZTP deployment, "set hostname " command does not push to FortiGate.
801415	FortiManager adds quotations to IP addresses when configuring trusted hosts for "switch-controller snmp-community" under the GUI's CLI Configuration.
801547	When removing an entry in the static route template, static route entries are shifted and the installation fails.
804142	Creating the "EMACVLAN" type Interface on FortiManager displays an error: "VLAN ID is required".
804502	Installation fails due to pushing the previous password expiration date to FortiGates.
804523	After creating SDWAN, IPSec, BGP & CLI template, the installation failed.
807771	FortiManager unsets the gateway settings in SDWAN template after upgrading ADOM from v6.4 to v7.0.
810936	After Upgrade, managed FortiAnalyzer on FortiManager does not display the Traffic logs under the *Log View* for HA devices.
811067	When creating/editing a blueprint, the *Firmware Enforcement* value is different from the default *Enforce Firmware Version* value.
812213	Default factory setting on FortiGate does not match with its default factory setting on FortiManager's DB. This causes status conflict if FortiGate added to the FortiManager using the "Add Model Device" method.
815901	The router static entries created by IPSEC template are deleted and re-created after upgrade.
818905	FortiManager unsets the certificate for "endpoint-control fctems" setting during the installation.
819710	FortiManager does not display the VDOMs opmode correctly.
820436	FortiManager displays an error "Failed to update device management data.", when adding a model device based on ZTP approach.

Bug ID	Description
821866	For FortiGates with FGSP (FortiGate Session Life Support Protocol) configuration, "ipsec-tunnel-sync" feature under the cluster-sync cannot be disabled.
823092	Not able to add multiple OU (Organization Unit) fields in the Certificate Templates.
823281	Changing Time/Schedule for scripts under the *Device Manager* makes the "OK" button grayed out.
824318	The *Description* column for interfaces displays wrong info (Up or Down).
826141	VLan interface cannot be created and mapped to a hardware switch interface on the FortiManager.
828122	"Device Detection" gets enabled by FortiManager during the installation.
828897	SD-WAN Monitor map doesn't load all devices.
829240	"Import CLI Script" feature is part of the "More" button entries under the *Device Manager*'s Scripts.
829404	SD-WAN Widget does not display any data for "Bandwidth Overview" and "Traffic Growth" under the *Managed Devices*' dashboard.
830085	FortiManager's GUI does not display the "Replacement Messages" Under System for its *Managed Devices* after visualizing it via "Feature Visibility".
830727	FortiManager-DOCKER platform does not support adding the FortiAnalyzer-DOCKER device.
831290	Failed to delete template group with "/" in their names.
831733	Unable to create any new entries for any of the sub tables of the BGP Router like Neighbors, Neighbor Groups, and etc. due to "datasrc invalid." error message.
831874	FortiManager's GUI keeps refreshing when clicking on the devices under the *Managed Devices*.
832321	Configuration changes on the AP/Switch/Extender settings do not apply on the device DB when these changes are created from the system template.
832599	When installing the "config system snmp community" settings to FortiGates, some of the entries are deleted.
832753	FortiManager does not install configurations from CLI Template group to FortiGates.
834947	"Resource-limits" proxy default value is missing under the *Device Manager*'s CLI Configurations.
835106	FortiManager cannot sync its devices with FortiAnalyzer when adding it to the *Device Manager*; it displays the error message "Serial number already in use".
835451	Editing SD-WAN/IPSec template with no actual changes removes all assigned devices.
836933	Changes on the External-Resource settings from ADOMs for specific VDOMs/FortiGates alter the External-Resource settings for other ADOMs and VDOMs.
838285	The DHCP server config under the FortiGate's interfaces does not work properly; it shows the

Bug ID	Description
	DHCP status as OFF and once fixed creates another identical entry under the DHCP Server.
838334	Unable to modify, install, or add members to Zone under the *System Template*.
839243	"Assigned to Device/Group" under the "System Templates" does not keep its config after FortiManager's upgrade.
839334	FortiManager does not allow empty value for *Interface Preference* as SD-WAN Rules under the *SD-WAN Templates*.
842923	Auto-update fails to sync FortiManager's device DB when interfaces are modified directly in the root VDOM of the FortiGates.
844979	Multiple issues under log settings for upload-time, FortiAnalyzer Cloud store-and-upload have been observed.
845552	FortiManager's GUI freezes after clicking "Upgrade Preview" and "Upgrade History" under *Device Manager* > *Firmware Templates*.
845656	When BGP is enabled and no IP address is defined for `set-ip-nexthop` under the `route-map` config, FortiManager tries to set the IP to 0.0.0.0, and this may break the BGP network.
847631	Failed to reload the FortiGate's configuration.
848485	"Enable FortiGuard DDNS" feature, under the DNS settings of each managed devices, cannot be unset.
850941	"Upgrade Now" page under the *Firmware Templates* does not show up when multiple devices are selected.
853061	Installation fails as FortiManager attempts configuring "allowas-in6" on neighbor when configuring router bgp via BGP template.
853810	Failed to edit the managed devices to modify the location.
854401	Unable to access to the FortiGates via SSH and GUI Console Widget once the FIPS mode is enabled from FortiManager.
855032	FortiManager displays the total devices/VDOMs count wrongly when split VDOM enabled on FortiGates.
855425	System Template and CLI Template config did not install to all model device FortiGates.
857039	After modifying the SSH Administrative Access for FortiGate's interface on *Device Manager*, FortiManager attempts to install the PPPOE's password again to the FortiGate.
858591	Editing the interfaces for any of the managed devices displays an error message.
859249	After upgrade, *Firmware Templates* under the *Device Manager* is blank. Even new entries cannot be created.
859638 860071	FortiManager's SD-WAN monitor does not display the Health Check status correctly.
860208	FortiManager's GUI does not save the http port number when configuring the "Explicit Web Proxy" under the *Device Manager*.

Bug ID	Description
861220	Leaving the SD-WAN member empty when configuring the SD-WAN using the template fails due to the syntax differences between FortiGate and FortiManager.
861238	SD-WAN Monitor, under *Device Manager*'s Monitors, displays an Unknown status icon (a grey question mark) for HA devices under the Map View.
863062	Modifying the SDWAN Overlay Template removes the corresponding BGP template network config.
863417	Proper IP configuration did not apply to FortiGates when provisioned via ZTP.
865583	"replacemsg-override-group" under the system's interface of managed devices is blank.
866243	The *SD-WAN Monitor* info for specific devices are not consistent with the map view SD-WAN interface status (based on performance SLA).
866920	System switch-interface member (internal) can not be used and provisioning template CLI scripts execute out of order.
870848	*SD-WAN Monitor* under *Device Manager* > *Monitors* does not display any FortiGate devices which are running in 6.2 version.
872865	FortiManager attempts to set a default value like "`system cluster-sync`" on FortiGate, and this causes installation failure.
874811	FortiManager tries to set the "set-ip-nexthop" to "0.0.0.0" during the installation.
874831	FortiManager attempts to install unknown and undesired static route when modifying or adding some new static routes.

FortiSwitch Manager

Bug ID	Description
818842	FortiManager displays "Failed loading data" for "Security Policy", "LLDP Profile", and "QoS Policy" features when editing ports in per-device mode FortiSwitch Management.
820167	Refreshing the FortiSwitch changes the status to *Unknown*.
820182	Using the *Export to Excel* feature for managed switches in *FortiSwitch Manager* exports a corrupted file.
829700	FortiManager shows errors while installing FortiSwitch configuration.
830099	*FortiSwitch Manager* displays the "Missing Switch ID or Platform Info" error.
833262	*FortiSwitch Manager* does not display the list of firmware images for the FSW 108F-FPOE model.
847846	*FortiSwitch Manager* does not display the correct switches and switchport status info.
868949	Installation fails as *FortiSwitch Manager* creates an alias name longer than the total limit 25 characters.

Global ADOM

Bug ID	Description
789164	Unable to delete the web rating override entries from ADOM Global Database.
835172	Global ADOM Assignment fails when assigning some profile groups.
835439	Global Policy assignment is not completed successfully due to some missing objects on Global ADOM.
838174	FortiManager does not provide a clear error message when Global IPS Header/Footer profile assignment fails.
842934	Global address group cannot be modified from FortiManager GUI.
847533	Unassigned Policy Package cannot be removed from Global ADOM.
868212	Assigning global policies to ADOMs by admins with access to specific ADOMs fails.

Others

Bug ID	Description
671471	In ADOM backup mode, when address objects are modified on FortiGates, modified objects are not imported into FortiManager.
707911	FortiManager should be able to assign VLAN interface to FortiExtender.
711100	FortiManager does not handle RMA and replaced FortiGates efficiently when ZTP has been used.
739219	FortiManager's timeout parameters cannot be set by users as it is hardcoded.
742819	Promote to global feature should not be possible since GLOBAL ADOM are not accessible in FortiManager Cloud.
745958	Unable to config ipsec tunnel using the ipsec tunnel template.
746516	Preferred Version cannot be saved for Managed Devices under the Firmware Images of FortiGuard Pane.
750242	FortiManager's DB in HA clusters are not properly synced together.
757524	FortiManager displays many "duplicate license for [FortiGate device's SN Number] copy AVDB to AVEN" error messages.
777028	FortiManager does not support the FortiCarrier-7121F.
782000	Unable to upgrade ADOM from v6.2 to v6.4 due to invalid value in CLI template.
788006	FortiManager consumes license count for the Admin Type VDOMs.

Bug ID	Description
793085	Sub Type Filter on Event Log search does not show any results, even if logs are present.
795624	FortiManager does not let users copy the contents of the "View Progress Report".
799378	FortiManager's admins are not able to run FortiManager's CLI scripts/commands from remote stations.
806522	Application websocket crashes and makes FortiManager's GUI unresponsive.
811018	FortiManager does not support copying objects from the Policy Packages and pasting them to the search field.
811798	Policy Package status not updated on the GUI after a successful installation.
816936	FortiManager does not support the FGT/FGC 7KE/7KF syntax.
818513	FortiManager does not support the FortiProxy v7.2.
820071	Upgrading the FortiOS/FortiGate firmware version via FortiManager did not complete successfully.
820248	Cloning same ADOM multiple times fails with error "Unknown DVM error".
820578	The "svc authd" process is consuming 100% of CPU.
820921	FortiManager displays incorrect device firmware versions for FortiSandbox and FortiMail.
821940	Static Route cannot be created under the *Device Manager* when FortiManager works in Workflow mode.
822642	FortiManager JSON API Documentation does not provide an accurate definition for the 'pkg' variable under the "/pm/config/adom/{adom}/pkg/{pkg}/" path.
823547	In Advanced ADOM mode, it is not possible to create a new VDOM in a new ADOM via JSON API request.
823872	FortiManager lost its access to GUI, if a same IP makes more than 250 connections to https admin port.
824316	FortiManager displays an error when "adom-integrity" is performed.
826881	FortiManager attempts to apply some changes to voice, video and interface configurations.
829726	Already existing CLI Templates cannot be modified after the upgrade.
830881	ADOM upgrade fails due to the ID of the sdwan applications; they are larger than the initial defined values.
831453	FortiManager shows an error message when multiple FortiGates are selected to be upgraded to the new version.
831616	FortiManager cannot install policy package when using Provisioning Templates as tasks got stuck.
833162	FortiManager does not support the FortiProxy 7.0.6.
833623	Estimated Bandwidth for Upstream & Downstream under the interfaces and Upload & Download values under the SD-WAN Monitor's table-view are displayed differently.

Bug ID	Description
835313	FortiManager displays many "duplicate license" messages for "copy AVDB to AVEN".
835748	FortiManager's GUI takes very noticeable time to load properly when navigating to Policy & Objects tab.
836489	Firmware Images under the FortiGuard for "All" or "Managed" devices display same list.
838949	Using the 'refresh' feature in the FortiExtender GUI does not refresh the stats of (RSSI, RSRP, etc.) of the associated devices.
839035	"Check License" under the FortiGuard's Licensing Status does not Keep the changes.
839586	FortiManager does not save applying the configuration of "Enable AntiVirus and IPS service for FortiDeceptor" under FortiGuard settings pane.
840068	Unable to export device stored FortiGuard signatures through tftp protocol.
840395	FortiManager does not support the FortiGate/FortiOS 6.4.11 Syntax.
841187	FortiManager does not support the FortiGate/FortiOS 7.0.8 Syntax.
841436	The `execute fmpolicy copy-adom-object` command does not support the device group feature.
845753	IPSec installation fails on Google Cloud Platform (GCP) ONDEMAND FortiGate.
850377	In Workflow Mode, when new session is created, the Policies disappear.
850467	Unprivileged Users might be able to disclose unauthorized information via API.
855840	'allowaccess' on interfaces completely removed on GCP ONDEMAND FortiGate.
857659	FortiManager did not download the "AI Malware Engine" Package from FortiGuard Server.
860817	In Workspace mode locking the ADOMs for cloning the ADOM objects is not required.
865200	Users encountered unsatisfactory performance of FortiManager due to several crashes on the "Application fmgd" process.
870893	Unable to install pp to FortiGates, after FortiManager's DB got restored.
874369	Upgrading FortiManager fails due to some invalid data for managed FortiExtender's Objects.
876425	FortiManager does not display the output of "execute dmserver showconfig".

Policy and Objects

Bug ID	Description
468776	FortiManager does not support FortiGate/FortiOS global scope (`g-`) objects.
585177	FortiManager is unable to create VIPv6 virtual server objects.
686150	FortiManager cannot import NSXT dynamic IP when VPN Objects are presented in *NSXT Manager*.

Bug ID	Description
688586	Exporting Policy Package to "CSV" shows "certificate-inspection" in the "ssl-ssh-profile" column even when the profile is not in use.
698838	"Download Conflict File" does not display all of the firewall objects conflicts when importing policy packages from FortiGate to FortiManager.
703408	FortiManager does not display the interface type Geneve for interface mapping.
704354	"Blocked Certificates" and "Server certificate SNI check" features cannot be configured on SSL/SSH profile.
707481	Deleting DNS filter profile does not delete the associated Domain filter.
711202	FortiManager does not support managing SAML user objects from *Policy and Objects*.
716892	Exporting to "Excel/CSV" does not include the value for fields "Log & Last Modified By".
724011	FortiManager needs to support multiple server certificate list in ssl/ssh profile.
731961	When FortiManager is working in the workspace mode, the installation for those FortiManagers with larger DB may take longer time to be completed.
738988	FortiManager does not detect the settings related to Web Cache Communication Protocol (WCCP) in SSLVPN Policies on the FortiGate.
741269	Unable to install configuration to FortiGates due to the error message "Resource temporarily unavailable".
742293	FortiManager, via ADOM 6.0, is not able to install "set logtraffic all" to proxy-policy with action deny.
747340	FortiManager does not support variables for source IP field under the Advanced Options of the Fabric Connectors' Threat Feeds.
752993	VPN IPSEC installation fails as phase1 settings on FortiManager are not consistent with the ones on FortiOS.
762392	The rating lookups does not return the correct category for the URL when it ends with "/" character.
765487	Install Wizard for Policy Package with no changes displays "No record found." which is not a clear message.
783195	FortiManager changes the "cert-validation-timeout" value to block when installing to the FortiGates.
787195	FortiManager skips the zone interface policy without displaying copy fail error message.
793240	FortiManager displays install failure due to adding "g-" prefix to the external-resource objects.
805211	Installation failed due to the wrong fsw vlan type for the default nac and nac_segment vlans.
810073	Fail to import the firewall policy due to the "interface mapping undefined" error message.
811715	FSSO dynamic addresses were visible on two address groups.
812886	On FortiManager, an internet-service-custom objects without protocol number or port-range

Bug ID	Description
	can be configured on firewall proxy-policy; however, FortiGate/FortiOS does not support this.
812909	FortiManager unsets the "bypass-watchdog" setting on FGT400E-Bypass.
814364	FortiManager does not support the FCT EMS prefix; therefore, policies with ZTNA Tags cannot be installed properly to the FortiGates.
814970	EMS Connector is not able to import Tags when Multi-Site enabled on EMS Server.
815281	SDN Dynamic Address object filter does not display the list properly.
815812	Installation failed because FortiManager tried removing the credentials for Amazon Web Services (AWS) type SDN Connector and enabling the "use-metadata-iam" feature.
816108	The "group-poll-interval" value for FSSO fabric connector cannot configured properly.
817220	FortiManager does not support the "userPrincipalName" as the common Name Identifier for LDAP Server configuration.
819847	FortiManager displays a false warning message "Duplicate Objects With Same Values" when creating the Firewall Objects' Service entries under *Policy & Objects*.
822843	FortiManager displays an error when using the access-proxy type VIP and normal VIP in firewall policies as they are both using the same external IP.
824770	FortiManager displays an error message when creating custom EMS Connector entries under the Fabric Connectors' Endpoint/Identity.
825411	Installation fails when an application group with category 32 (unknown applications) is configured on FortiManager, even though this category is accepted on the FortiGate.
825530	Explicit web proxy policy does not allow selecting any source address objects.
825873	FortiManager does not support FortiGate/FortiOS global scope (g-) objects.
826928	During the installation, FortiManager attempts to remove the physical ports which are members of the virtual-switch config.
826946	FortiManager does not show anything to install on FortiGates even though the Policy Package has been modified.
827242	For Policies under the Advanced Options, "custom-log-field" uses Names instead of IDs.
827815	Removing "FortiClient EMS" entries under the "Endpoint/Identity" of "Fabric Connectors" displays error messages.
830043	Creating the Custom IPv6 service where icmp code is not configured causes the Policy Package to get into a conflict state.
830502	FortiManager fails to create the CSV for Policy Package.
831225	Cloning a policy with VIP referencing SDWAN member causes subsequent installs to fail.
831273	FortiManager does not allow deleting the entries for "server-info" under the log "npu-server".
831407	NSX-T connector configuration does not display "VM16" and "VMUL" types.

Bug ID	Description
831484	FortiManager was not able to connect to the "NSX-T Connector" and several "Application connector" failures have been observed.
832962	If Firmware Template status is "Unknown", FortiManager allows installing the Policy & Packages repeatedly to the FortiGates.
834102	Editing Fortinet Single Sign-On Agent entry under the Endpoint/Identity removes FSSO user groups from the Firewall Policy.
834401	Upgrading ADOMs do not complete if there are some empty values for "profile-type" and "utm-status".
834447	Objects are not visible in the 'Addresses' tab when per-device mapping feature is enabled.
834558	Installing tunnel interfaces which are created by ipsec template fails.
834806	Installation fails due to extra back slashes when installing the custom IPS signatures to the FortiGates.
835079	Detail of the "Firewall Security Policy" when running the Policy Package Diff does not display data for all fields.
836103	FortiManager pushes old internet-service-names "Facebook" instead of "Meta".
836783	FortiManager changes the "use-metadata-iam" value for the SDN connectors.
837555	Connector's Service Name, after FortiManager's upgrade, does not display the correct name.
838533	SASE zone cannot be removed from SDWAN Template.
838648	"Rename objects to import" inconsistency with "datasrc duplicate" error.
841492	FortiManager unsets the system HA settings after pushing an unsuccessful installation Policy Package to FortiGates.
843765	FortiManager does not display the proxy address members under the proxy address group.
844985	Per-device mapping is not supported for Virtual Server with "IP" type.
845638	"ztna-ems-tag"s created on FortiGates are not same as ZTNA Tags created on FortiManager; hence, the installed tags from FortiManager to FortiGates, used in firewall does not police the traffic properly.
847932	Hit count for a policy package does not always match the total count of all installation targets.
848666	"Install Device" task stuck without any progress when installing the templates and firewall policies to the FortiGates.
849470	When creating a new firewall policy via API Request the "global-label" option is skipped.
850204	Installing an AWS connector with Metadata IAM enabled displays an error message.
851331	Cloning Firewall Addresses under the Firewall Objects does not clone the "Add To Groups" entries.
853815	New created LDAP users are displayed based on the <CN> attributes and not the <sAMAccountName> attributes or User ID parameters.

Bug ID	Description
853851	FortiManager displays all the FortiTokens for the FortiToken settings under the User Definition even though some of them are already assigned.
858183	After firmware's upgrade, virtual wire pair interfaces are missing in virtual wire pair interface policy.
859217	Rearranging the Destination NAT (DNAT) objects whose names contain special characters displays an error message: "object does not exist".
862727	Policy Package installation failed due to the error "native vlan must be set" message.
862839	Cloning the Policy Packages on FortiManager creates the duplicate UUIDs.
863882	'Last Modified Time' field is empty when exporting Policy Packages to Excel.
866826	Failed to modify Virtual Server addresses in Firewall Polices with Deny Action.
870688	Editing the "Install On" changes the Policy status to "Modified" for all FortiGates existing on that rule.
873006	Firewall Address entries cannot be modified and GUI displays an error message: "Objects already exists."
873896	Unable to remove "(null)" objects under "endpoint-control".
874188	Installation fails due to FortiManager's attempts to remove the "`endpoint-control fctems`" entries.
875980	FortiManager unsets EMS connector Serial Number and the tenant-id during the installation.

Revision History

Bug ID	Description
513317	FortiManager may fail to install policy after FortiGate failover on Azure.
722332	For AP Profile change, installation preview may show No Entry.
738376	Config revision diff check may highlight the differences in config even though both revisions are exactly the same.
809191	Configuration change of HA-logs setting is not reflected in the revision history.

Script

Bug ID	Description
795639	Any commands after the "set secret" command in the "switch-controller custom-command" configuration is displayed in a form of encrypted strings.

Bug ID	Description
808398	"View script executing history" displays scripts related to other ADOMs.
817172	Running scripts to add static route has been failed due to the "duplicate of static route" error.
821778	Using scripts do not create the ssl-ssh-profile with certificate inspection mode; instead, it sets the value to deep-inspection mode.
829918	Scripts containing meta variables do not work after upgrade.
833285	Installation failed when executing multiple Jinja scripts.

Services

Bug ID	Description
779997	When upgrading the multiple FortiGates at the same time from the "Firmware Upgrade" feature, it does not let users to click "OK".
783422	FortiManagers configured in closed network do not support keeping the multiple entitlement copies in FortiManager's Database.
820400	In closed network scenario, when FortiManager loses connection to Local FortiGuard, eventually, licenses become invalid.
827982	Downstream FortiManagers cannot get all the FDS/FGD packages from upstream FortiManagers in cascade mode network design.
837942	In cascade mode, FortiManager as local FortiGaurd Server does not download IPS signature for extended database.

System Settings

Bug ID	Description
753204	Admins of a specific ADOM are able to see tasks of others ADOMs.
777153	FortiManager displays an error when setting up a "Remote Authentication Server" with "No Certificate" option.
801580	Fail to use the Online Help as it does not use the proxy config setting which has been set for FortiManager/FortiAnalyzer.
815728	FortiManager takes very long hours to rebuild the HA Cluster back to synchronization status.
822776	Query Distinguished Name does not display the LDAP users in FortiManager when Secure connection is enabled.
823898	FortiManager does not use all of the configured "ssl-cipher-suites" under its "system global"

Bug ID	Description
	settings.
825078	New admins with ADOM only access cannot see the previously assigned header and footer policies on that ADOM.
829751	Installation tasks got stuck at 0% and failed to start any new installation tasks.
830242	FortiManager in Advanced Mode does not show the number of allowed VDOMs correctly.
833989	Cannot set/change the service access settings on the interfaces when the language is not set to English/French.
841782	In Workflow mode, admins are not able to click on the "Approve this request" received from the emails as it displays "Unable to complete action" or "Invalid adom name" error messages.
841931	When FortiManager works in Workspace Mode, users are able to disable "Per-Device Mapping" without locking the ADOMs.
843520	After firmware upgrade, FortiManager/FortiAnalyzer's HA Cluster is broken and Access to the Secondary fails.
848934	SNMPv3 does not work properly on FortiManager and FortiAnalyzer.
850469	Radius group attribute filter does not work with Microsoft NFS.
851029	FortiManager's HA cluster breaks after upgrading the FortiManager.
853353	SDWAN Monitor Map does not show up when admin profile has been set to "None" for *System Settings*.
862592	Upgrading FortiManager did not finish and GUI displays the "Temporarily Unavailable" message.
862814	Event logs did not log FortiManager admins and their actions on managed devices.
864041	SNMPv3 stopped working after upgrading the FortiManager.
864931	Unable to login into FortiManager using TACACS and Radius credentials.

VPN Manager

Bug ID	Description
762401	FortiManager is unable to preserve the Specify custom IP ranges option for SSL VPN Address range setting.
831076	Static Route (Protected Subnet of the HUB) is not installed to Spoke during install with HUB and Spoke Dial-up VPN setup.
866248	Configuring a new mesh VPN using *VPN Manager* failed due to the extra character in the encryption method for Phase2.

Common Vulnerabilities and Exposures

Visit https://fortiguard.com/psirt for more information.

Bug ID	CVE references
872711	FortiManager 7.2.2 is no longer vulnerable to the following CVE-Reference: • CVE-2023-22642

Known Issues

The following issues have been identified in 7.2.2. To inquire about a particular bug or to report a bug, please contact Customer Service & Support.

AP Manager

Bug ID	Description
861941	FortiManager attempts to install "`arrp-profile`" even if "`darrp`" is disabled.
881548	Unable to install successfully when creating a SSID using its default value.
884233	FortiManager displays the AP critical security vulnerability info even after FortiAPs are being upgraded.
889811	Under WIFI and switch controller for Managed FortiAPs, there is not any LLDP info found.

Device Manager

Bug ID	Description
817346	Editing interface with normalized interface mapping displays some unnecessary messages for mapping change.
837213	Browser may crash when clicking "*view diff*" to compare with current device config. This might happen due to a slow network. **Workaround**: Use "*show diff only*" from Revision History instead of checking it from "Out of Sync" devices list.
876040	Status of Certificates is displayed as "pending" under the System's Certificates.
879833	Adding a model device with variable to FortiManager displays an error message: "a[i].replace is not a function".
881148	SAML user - retrieve/refresh/install and device authorization fail from GUI after upgrading FortiManager to 7.2.2. **Workaround**: Set `rpc-permit` to `read-write` for SSO user on SP FortiManager.
881308	The default value of the "`router.static.vrf`" leads to installation failure when attempting to install blackhole routes to FortiGates.
885454	After upgrading FortiManager, certificates for FGT 1100E's are missing from the *Device Manager*.

Bug ID	Description
886917 888930	FortiManager's ipsec templates remove the sdwan member and bgp neighbor attached to an ipsec interface. This causes the sdwan member to be removed even when it's used.
888658	Editing DHCP Settings of a FortiGate interface displays the following error message: "You have no permission to access this device/vdom".
889566	"View Config" in *Device Manager* > *Revision History* does not display full configuration of the managed device.
891216	Unable to edit/save interface with DHCP relay enabled.
891341	Installation fails due to the Copy failure error; system template created with some empty string values which are assigned to devices.
891967	When management VDOM is non-root and has been assigned to a different ADOM, FortiManager displays the error, "Can not access device global setting if management VDOM is not in current ADOM".
893592	Exporting the Device List to CSV and Excel file doesn't include the FortiAPs and FortiSwitches info.
896998	Unable to get access to the Certificates via Device Manager > DEVICE_NAME > VDOM_NAME > System.
897863	After deselecting the "`allow-dns`" feature under the application control list, the changes cannot be saved.
899903	FortiManager GUI does not list all NTP interfaces.
912833	Adding FortiGates with Open Authentication (OAuth) Method, Fortinet Security Fabric dialog box does not display the FortiManager's related info.

FortiSwitch Manager

Bug ID	Description
872802	FortiManager automatically sets "`default`" as dnsfilter-profile under dns-server for fortilink interface.
890205	Selecting multiple ports to "*Edit*" is not possible as it is greyed out.

Global ADOM

Bug ID	Description
826522	Unable to remove global object from Global Database in workspace mode.

Bug ID	Description
	Workaround: Unlock & lock the Global ADOM prior to deleting the Global Object and assigning changes to local ADOMs.

Others

Bug ID	Description
703585	FortiManager may return 'Connection aborted' error with JSON API request.
713714	The schedule for firmware upgrade for FGTs does not work if the upgrade request is issued from the CLI, instead firmware upgrade starts immediately. **Workaround**: Use firmware upgrade templates in the GUI.
777831	When FortiAnalyzer is added as a managed device to FortiManager, *Incident & Event* Tile will be displayed instead of the *FortiSoC*.
802922	The application "`newcli`" process crashes when the "`diagnose cdb upgrade check +all`" command runs.
814425	Sorting FortiExtenders by Network, RSSI, RSRP, RSRQ, and SINR does not work properly.
829046	After the upgrade, some of the metadata variables are missing.
838638	FortiGates are upgraded successfully via FortiManager's Group Firmware upgrade feature; however, the task monitor displays "Image upgrade failed" for some of the FortiGates.
851586	FortiManager displays "invalid scope" errors when running the "`diagnose cdb check policy-packages`" command.
869955	BGP Template route map option does not support Meta Variables.
871608	Unable to retrieve routing information from FortiGate via FortiManager when there is a large routing table.
875006	When clicking on the warning message, which indicates critical security vulnerabilities, a list of all types of security vulnerabilities is displayed.
883548	FMG/FAZ is forcing its users to upgrade the Firmware version upon login.
891869	FortiManager wrongly recommends lower version for upgrade the FortiGates.
895982	Admin with a Super User profile is not able to create the Firmware Template when FortiManager is working in the Workflow mode.
899570	Unable to add the "FortiGateRugged-60F" FGT to the FortiManager.
899750	ADOM upgrade makes the Policy Packages status modified.
906533	Group options, when creating/editing the workflow approval group, displays wrong info.

Policy & Objects

Bug ID	Description
739489	It's not possible to enable NAT with Outgoing Interface Address by directly right-clicking on the NAT section of a firewall policy. **Workaround**: Configure NAT by editing the firewall policy.
751443	FortiManager displays policy installation copy failures error when ipsec template gets unassigned. **Workaround**: Instead of unassigning IPSec template, modify IPSec template, replace the reference to IPSec tunnel interface with another interface. Please ensure a fresh FortiManager's backup is created prior to any changes.
774058	Rule list order may not be saved under *File Filter Profile*.
803460	"User Definitions" entries under the "User & Authentication" cannot be removed from FortiManager.
821114	EMS ZTNA Tags in FortiManager and FortiGate are using different naming convention; therefore, installing the policies with those tags to FortiGates do not work.
827416	FortiManager does not display any copy failure errors when utilized objects do not have any default values or per-device mapping.
845022	SDN Connector failed to import objects from VMware VSphere.
846634	GUI does not allow to edit the custom Application and Filter Overrides.
862014	FortiManager is purging 'replacement message group custom' configuration after install verification fails.
866724	Copy Failed error has been observed with the error message "Virtual server limit reached!"; this limit is 50 for FGT AWS ONDEMAND.
867809	During installation, FortiManager unsets status for the proxy policies.
875547	Policy & Package cannot be imported, if the type of firewall address in FortiGate is "`interface-subnet`" and subnet's value is different with its value on FortiManager.
877477	Domain Name Threat Feeds are not available in *DNS Filter > Remote Categories*.
880359	FortiManager is purging 'replacement message group custom' configuration after install verification fails.
880431	Unable to define Exempt IP in IPS Sensor.
880575	When using the "reinstall policy" option to install to devices with different policy packages, the corresponding event log shows the same policy package pushed to all devices.
881634	When multiple VDOMs are selected for installation using the Re-install Policy feature, FortiManager only applies "`re-install policy`" for one VDOM from each devices.
881857	Multiple security console Application crashes have been observed during the Policy Package installation when static router template and router static entry in device db are used.

Bug ID	Description
882477	Error Message "Object already exists" is displayed when editing per device mapping for Address Group.
882996	Unable to install to FortiGates when using null values for "`local-gw6`" and "`remote-gw6`".
883527	Install Preview does not display any info during the installation when using device groups in PP Installation Targets.
885827	FortiManager does not save and keep the selected "collapse all" mode for the policy package.
885992	Duplicate section names are created for policy package when ViewMode interface pair View is selected.
886370	FortiManager does not sort by interface per view results correctly; the results are not displayed in alphabetical order.
886911	FortiManager is attempting to modify replacement messages after upgrade, and this leads to installation failure.
887278	Installation failed due to the limit on max entery for "`endpoint-control fctems`".
889563	FortiManager, for ADOM version 6.4, does not support Creating, Importing, or Inserting Above and Below actions for a deny policy with a "Log Violation Traffic" disabled. **Workarounds**: • To Insert, use copy & paste instead of the using Insert Above/Below. • To Create, either run script to create log disabled deny policy or enable log traffic first, and then edit the policy in order to disable and save it.
891832	The install preview for policy package being used by multiple FortiGates is taking some time to load.
891996	"Find and Replace" feature does not display the entries correctly and it does not allow any changes.
895979	FortiManager attempts setting the Zone as the interface for firewall policy during the installation.
899339	FortiManager does not seek for confirmation when deleting an object from firewall policy.

Script

Bug ID	Description
876917	"Capture Diff to a Script" does not work properly. It does not display the changes.

System Settings

Bug ID	Description
825319	FortiManager fails to promote a FortiGate HA Slave member to the Primary.
873078	FortiManagers HA cannot be configured as the initial sync never completes.
884168	FortiManager suggests wrong versions to upgrade FortiGates in order to resolve the PSIRT Vulnerability.
884396	The firmware upgrade notification on the FortiManager and FortiAnalyzer keeps appearing continuously after each login.
884848	FortiManager HA is not syncing after upgrade as the synchronization between the cluster units never completes.
888374	Admin user's ADOM setting cannot be synced to secondary when `adom-access` is set to `specify`.
894366	Any changes related to "lan" interface on FGT 40F, where the role is defined as "LAN", FortiManager tries installing firewall address "lan address" with type interface-subnet linked to interface "lan". The Install Verification fails for "lan address" as "entry not found in database".

VPN Manager

Bug ID	Description
784385	If policy changes are made directly on the FortiGates, the subsequent PP import creates faulty dynamic mappings for VPN manager. **Workaround**: It is strongly recommended to create a fresh backup of the FortiManager's configuration prior to this workaround. Perform the following command to check & repair the FortiManager's configuration database: `diagnose cdb check policy-packages <adom>` After running this command, FortiManager will remove the invalid mappings of vpnmgr interfaces.
798995	It's not possible to delete an SSL VPN portal profile from FortiManager GUI if the profile has been already installed.
857051	Installing a policy package with IPSec VPN to FortiGates fail with the following error: "TCL error (The remote gateway is a duplicate of another IPsec gateway entry)".
888272	Single entry of SSLVPN settings cannot be selected under *VPN Manager*.

Appendix A - FortiGuard Distribution Servers (FDS)

In order for FortiManager to request and retrieve updates from FDS, and for FortiManager to serve as an FDS, please configure the necessary settings on all devices between FortiManager and FDS, or between FortiManager and FortiGate devices based on the following items:

- FortiManager accesses FDS for antivirus and attack updates through TCP/SSL port 443.
- If there is a proxy server between FortiManager and FDS, FortiManager uses port 80 to communicate with the proxy server by default, and connects to the proxy server using HTTP protocol.
- If FortiManager manages a FortiGate device located behind a proxy server, the proxy server permits TCP/SSL traffic to pass through port 443.

FortiGuard Center update support

You can configure FortiManager as a local FDS to provide FortiGuard updates to other Fortinet devices and agents on your network. The following table lists which updates are available per platform:

Platform	Update Service	Query Service
FortiGate	✓	✓
FortiADC	✓	
FortiCache	✓	
FortiCarrier	✓	✓
FortiClient	✓	
FortiDeceptor	✓	✓
FortiDDoS	✓	
FortiEMS	✓	
FortiMail	✓	✓
FortiProxy	✓	✓
FortiSandbox	✓	✓
FortiSOAR	✓	
FortiTester	✓	
FortiWeb	✓	

Appendix B - Default and maximum number of ADOMs supported

This section identifies the supported number of ADOMs for FortiManager hardware models and virtual machines.

Hardware models

FortiManager supports a default number of ADOMs based on hardware model.

Some hardware models support an ADOM subscription license. When you purchase an ADOM subscription license, you increase the number of supported ADOMs. For example, you can purchase an ADOM subscription license for the FMG-3000G series, which allows you to use up to a maximum of 8000 ADOMs.

Other hardware models do not support the ADOM subscription license. For hardware models that do not support the ADOM subscription license, the default and maximum number of ADOMs is the same.

FortiManager Platform	Default number of ADOMs	ADOM license support?	Maximum number of ADOMs
200G Series	30		30
300F Series	100		100
400G Series	150		150
1000F Series	1000		1000
2000E Series	1200		1200
3000G Series	4000	✓	8000
3700G Series	10,000	✓	12,000

For FortiManager F series and earlier, the maximum number of ADOMs is equal to the maximum devices/VDOMs as described in the FortiManager Data Sheet.

Virtual Machines

FortiManager VM subscription license includes five (5) ADOMs. Additional ADOMs can be purchased with an ADOM subscription license.

For FortiManager VM perpetual license, the maximum number of ADOMs is equal to the maximum number of Devices/VDOMs listed in the FortiManager Data Sheet.

FortiManager VM subscription and perpetual licenses are stackable.

www.fortinet.com